Multiclass Classification with Potential Function Rules: Margin Distribution and Generalization

Fei Teng\textsuperscript{a,c}, Yixin Chen\textsuperscript{a,c,1}, Xin Dang\textsuperscript{b,c}

\textsuperscript{a}Department of Computer and Information Science, \textsuperscript{b}Department of Mathematics, \textsuperscript{c}The University of Mississippi, University, MS 38677, USA.

Abstract

Motivated by the potential field of static electricity, a binary potential function classifier views each training sample as an electrical charge, positive or negative according to its class label. The resulting potential field divides the feature space into two decision regions based on the polarity of the potential. In this paper, we revisit potential function classifiers in their original form and reveal their connections with other well-known results in the literature. We derive a bound on the generalization performance of multi-class potential function classifiers based on the observed margin distribution of the training data. A new model selection criterion using a normalized margin distribution is then proposed to learn “good” potential function classifiers in practice.

Keywords: Multiclass classification, consistent classification rules, potential function rules, kernel rules, margin distribution, large margin classifiers, generalization bounds, model selection

1. Introduction

For thousands of years, various civilizations have observed “static electricity” where pieces of small objects with the same kind of electricity repelled each other and pieces with the opposite kind attracted each other. In pattern recognition and machine learning, potential function rules were motivated from the underlying property of static electricity to predict the

\footnote{To whom all correspondences should be addressed. Tel. 1-662-915-7438; Fax. 1-662-915-5623. ychen@cs.olemiss.edu}

Preprint submitted to Pattern Recognition April 13, 2011
unknown binary nature of an observation, a problem commonly known as
binary classification. Potential function rules were originally studied by Aizer-
erman, Braverman, Rozonoer, and several other researchers in the 1960’s ([1, 2, 3, 4, 10, 17, 18]). In its simplest form, a potential function rule puts
a unit of positive electrical charge at every positive observation and a unit
of negative electrical charge at every negative observation. The resulting pot-
tential field defines an intuitively appealing classifier: a new observation is
predicted positive if the potential at that location is positive, and negative
if its potential is negative.

In this paper, we revisit potential function rules (PFRs) in their original
form and reveal their connections with other well-known results in the lit-
erature. We derive a bound on the generalization performance of potential
function classifiers based on the observed margin distribution of the training
data. A new model selection criterion using a normalized margin distribution is then proposed to learn “good” potential function classifiers in practice.
There is an abundance of prior work in the field of pattern recognition and
machine learning. It is beyond the scope of this article to supply a complete
review of the area (for more comprehensive surveys on various subjects, the
reader is referred to Devroye et al. [30], Duda et al. [35], Bishop [14] for pattern
recognition, to Schölkopf and Smola [58], Shawe-Taylor and Cristianini [59]
for kernel methods, to Anthony and Biggs [5], Kearns and Vazirani [45] for
computational learning theory, and to Mitchell [53], Hastie et al. [42], Vap-
nik [65] for machine/statistical learning). Nevertheless, a brief synopsis of
some of the main findings most related to this article will serve to provide
a rationale for the use of PFRs in pattern recognition and machine learning
applications.

1.1. The Bayesian Decision Theory and Plug-In Decisions

A multiclass classification problem aims at foretelling the unknown nature
of an observation. More formally, an observation is a $d$-dimensional vector
of numerical measurements denoted as $\mathbf{x} \in \mathbb{R}^d$. The unknown nature of the
observation, $z$, takes values in a finite set $\mathbb{K} = \{1, 2, \ldots, K\}$, the set of class
labels. A mapping $f : \mathbb{R}^d \rightarrow \mathbb{K}$, which is named a classifier, predicts the class
label of an observation.

Does there exist an “optimal” classifier for a given classification task?
Under a probabilistic setting, the Bayesian decision theory [11, 13] gives an
affirmative answer – the Bayes decision rule (or called the Bayes classifier). If
the pair of observation and its nature, $(\mathbf{x}, z)$, is a random variable with a joint
probability distribution \( p(x, z) \), the Bayes classifier, \( f^* \), selects the class label for an observation \( x \) as \( f^*(x) = \arg\max_{z \in K} \Pr(z|x) = \arg\max_{z \in K} p(x, z) \). The optimality of \( f^* \) is defined by the minimum probability of error, i.e., \( \Pr[f^*(x) \neq z] \leq \Pr[f(x) \neq z] \) for any \( f : \mathbb{R}^d \to K \), which is well-known as the Bayesian probability of error. This probability measures the ‘hardness’ of a classification problem. It can theoretically be evaluated if the joint distribution is known, but the calculation may be (and usually is) intractable in practice due to the min operator inside the integral. Several tight bounds were proposed in the literature for computational approximations of the Bayesian probability of error [25, 41, 6].

The crux of the Bayesian approach is the difficulty of determining the joint distribution. Plug-in decision [30] is a natural way of applying the Bayesian classification in practice, where an approximated Bayes classifier is constructed using an estimated joint distribution. Depending upon the way in which the joint distribution is estimated, plug-in decision rules fall roughly into the parametric approaches and the nonparametric approaches.

In a parametric approach, the unknown joint distribution is described by a set of parameters based on certain structural assumptions, e.g., conditional independence of attributes within each class [49, 34, 15, 50], mixture of Gaussians [46, 61, 19], and mixture of Bernoullis [61]. The values of the parameters are obtained by optimizing a loss function, e.g., a likelihood function. In many applications, a parametric approach presents an efficient means of incorporating prior knowledge about the data. For example, Hofmann et al. [43] used a latent variable model (aspect model) to remove the statistical dependence among words in a document for textual data. Barnard et al. [7] explored several generative models to describe statistical relevance between images regions and associated texts. Veeramachaneni and Nagy [66] studied the interpattern dependence, named style context, for Optical Character Recognition. Intraclass style (statistical dependence between patterns of the same class in a field) and interclass style (statistical dependence between patterns of different classes in the same field) were formalized to derive style-constrained Bayesian classification.

The performance of a plug-in decision rule is determined by the quality of the estimated joint distribution. Ben-Bassat et al. [12] analyzed the sensitivity of Bayesian classification under multiplicative perturbation on the joint distribution. Devroye [26] presented a more general result showing that if the estimated posterior probability is close to the true posterior probability in \( L_1 \)-sense, the error probability of the plug-in decision rule is near
the Bayesian probability of error. Nevertheless, does the error probability converge to the Bayesian probability of error if more training samples are obtained to approximate an arbitrary joint distribution? This is a question regarding the universal consistency of a classification rule. Loosely speaking, a universally consistent rule guarantees us that taking more samples suffices to roughly reconstruct an arbitrary, fixed, but unknown distribution, hence to asymptotically achieve the optimality. While parametric approaches are efficient, in general they are not universally consistent.

In 1977, Stone proved the existence of a universally consistent rule [60]. He showed that any $k$-nearest neighbor classifier is universally consistent if $k$ is allowed to grow with $n$, the sample size, at a speed slower than that of $n$. Since then several rules have been shown to be universally consistent including histogram rules [37] and kernel rules [30]. We put these approaches under the category of nonparametric plug-in decisions because of the underlying nonparametric estimation of joint distributions. Representing all the data with a nonparametric model is sometimes preferred over summarizing it with a parametric model because of the rich detail held by very large data sources [40].

1.2. Classifier Selection and Complexity Regularization

Universal consistency describes the asymptotic behavior of a classifier, i.e., the number of training samples goes to infinity. For real-life problems, however, the size of a training set is finite and, usually, fixed. This leads to a basic question in classifier design: how do we select a classifier, which performs well on future examples, from a given set of classifiers based on a given finite training set? Two basic principles were investigated in the literature for classifier selection: empirical risk minimization [63] and complexity regularization [51].

In order to achieve good generalization performance, the empirical risk minimization principle seeks for a classifier that minimizes the training error (empirical risk). Vapnik and Chervonenkis presented a theoretical ground for empirical risk minimization [63]. It was shown that if the ‘capacity’ of $\mathcal{C}$, the set of classifiers to choose from, is sufficiently restricted, minimizing the empirical risk guarantees a classifier whose performance is close to that of the best classifier in $\mathcal{C}$. Here the capacity of $\mathcal{C}$ is defined by the VC-dimension of $\mathcal{C}$. The above result reveals two competing factors in classifier selection. On one hand, a low capacity model set may not contain any classifier that generalizes well. On the other hand, too much freedom may over fit the
data resulting a model behaving like a refined look-up-table: perfect for the training data but poor on generalization.

This suggests that a classifier, built on a finite training set, generalizes the best if the right tradeoff is found between the training accuracy and the capacity of the model set. Complexity regularization applies the above idea to search for a classifier that minimizes the sum of empirical risk and a term penalizing the complexity \[64, 8, 51, 9, 16\]. Amongst various definitions of the penalty term, margin-based approaches received broad attention in the literature. A series of results were obtained that exhibit the intrinsic connection between generalization and different measures of margin distribution (e.g., maximal margin, margin percentile, soft margin) \[65, 48, 59, 55, 39\]. These theoretical results led to the discovery of new learning algorithms (e.g., support vector machines \[65\], margin distribution optimization \[36\], large margin multiple-instance learning \[21\], margin trees \[62\], large margin semi-supervised learning \[67\], dissimilarity-based learning \[54\], similarity-based learning \[52, 22\], large margin nearest neighbor classification \[69, 44\], large margin conditional random fields \[47\], and new interpretations of known learning algorithms (e.g., boosting \[57, 56\], additive fuzzy systems \[20\]).

Classifiers derived from complexity regularization are not necessarily consistent. Lugosi and Zeger \[51\] presented a sufficient condition for universal consistency of a particular method of complexity regularization, structural risk minimization, using Vapnik-Chervonenkis complexity classes \[65\]. As discussed in Section 1.1, several nonparametric plug-in decision rules are universally consistent. A question arises naturally: Can we combine complexity regularization with a universally consistent nonparametric plug-in decision rule to improve the generalization performance thereof? This is the question that we attempt to address in this article. In particular, we focus on the regularization of multiclass PFRs based on a margin distribution.

1.3. A Historical Timeline of Potential Function Method

Potential function method was invented by Russian researchers in the 1960’s to model a general function reconstruction problem \[1, 2, 3, 4, 10, 17, 18\]. Various algorithms were proposed to tackle the reconstruction problem for specialized purposes. In a series of three articles, Aizerman, Braverman, and Rozonoer proposed algorithms using a potential function for binary classification \[1\], estimation of the posterior probability of binary classes \[2\], and approximating a functional relationship \[3\].
Under the specific problem settings, various convergence results were obtained [1, 17, 18, 4]. In [1], a learning method for potential function classifier was shown to converge in finite number of iterations when the two classes are separable by the given family of potential functions. Under the same assumption, a probabilistic bound was derived in [4] that can be used as a termination condition for the training process. The bound is essentially a sample complexity bound in computational learning theory [45]. Braverman and Pyatnitskii [17] established criteria for the choice of potential function used in convergent learning algorithms. In a later work, they estimated the rate of convergence [18].

In the simplest form, a binary PFR views each training sample as an electrical charge, positive or negative according to its class label. The resulting potential field divides the feature space into two decision regions based on the polarity of the potential. In the original formulation of PFR [1, 17], the electrical charge of each training sample is assigned a weight coefficient. In this article, we consider a simpler form with uniform weights. The basic idea of binary PFRs can be generalized to the multiclass scenario, in which a potential function is defined for each class using the training observations within that class. A new observation is then assigned a label corresponding to the class of the highest potential value. In addition to the intuitive appealingness, good scalability is a main advantage of PFRs in applications of a ‘dynamic’ nature, i.e., the structure of the problem may vary over time. Adding new classes does not affect the existing potential functions. Removing or merging classes influence only the potential functions of the classes involved in the operation.

1.4. An Overview of the Article

The contributions of this article are given as follows:

- Connections of PFRs with the Bayes decision theory. Given charge density functions a priori, we present conditions under which a PFR is essentially optimal under the framework of the Bayesian decision theory. We then look into a more practical scenario where a PFR is built from a given set of training observations with unknown but fixed charge density functions. We show that a PFR is, in this case, equivalent to a plug-in decision rule using kernel density estimation, hence universally consistent.
• A new generalization bound for PFRs. We discuss the classifier selection for PFRs using complexity regularization. An upper bound on the generalization performance for PFRs is derived using a margin distribution.

• A simple classifier selection method for PFRs. Motivated by the above generalization bound, we propose a simple kernel selection method using a normalized margin distribution. Extensive experimental results on artificial data and real applications demonstrate the competitive performance of the proposed framework.

The remainder of the paper is organized as follows: Section 2 discusses PFRs from the perspective of the Bayesian decision theory. Conditions under which PFRs are equivalent to Bayes decision rules are presented. Section 3 shows a connection between a PFR and a plug-in decision rule using kernel density estimation. Section 4 presents a generalization bound for PFRs based on a margin distribution. Motivated by this bound on the generalization performance of PFRs, we propose in Section 5 a model selection method using a normalized margin distribution. In Section 6, we explain the experimental studies conducted and demonstrate the results. We conclude in Section 7.

2. Potential Function Rules and The Bayes Decision Theory

We start with a brief review of electrostatic potential functions [38]. We then introduce the general form of binary potential function classifiers. Finally, we demonstrate connections between PFRs and the Bayes classifiers.

2.1. Potential Function Rules

Given a positive point charge at location \( y \), the electrostatic potential at location \( x \) is proportional to \( \frac{1}{\| x - y \|} \), which is called the electrostatic point potential function. For a ‘cloud’ of positive charges with density \( \rho_+ \) over a space \( X \), the electrostatic potential function \( \Phi \) is, modular a constant scale factor,

\[
\Phi(x) = \int_{X} \frac{\rho_+(y)}{\|x - y\|} dy.
\]

Therefore, if \( \rho_+ \) and \( \rho_- \) are respectively the charge density of positive and negative charges over \( X \), the electrostatic potential function \( \Phi \) is, modular a
constant scale factor, defined as

\[ \Phi(x) = \int_X \frac{\rho+(y)}{||x-y||} \, dy - \int_X \frac{\rho-(y)}{||x-y||} \, dy. \]

The above electrostatic potential function can be generalized by replacing the electrostatic point potential function with a general point potential function \( \psi : X \times X \to \mathbb{R} \):

\[ \Phi(x) = \int_X \rho+(y)\psi(x,y) \, dy - \int_X \rho-(y)\psi(x,y) \, dy. \] (1)

Note that the electrostatic potential at a location \( x \) is not well defined if \( x \) falls in the support of \( \rho+ \) or \( \rho- \) due to the fact that \( \frac{1}{||x-y||} \) is \( \infty \) when \( x = y \). This limitation, however, can be avoided by a general potential function (1) with a proper choice of the point potential function \( \psi \).

Given \( \rho+ \) and \( \rho- \), let \( Q+ \) and \( Q- \) be the total positive charge and negative charge, respectively:

\[ Q+ = \int_X \rho+(x) \, dx, \quad Q- = \int_X \rho-(x) \, dx. \]

We normalize the potential function (1) by the sum of the total positive and total negative charges:

\[ \frac{\Phi(x)}{Q+ + Q-} = \frac{Q+}{Q+ + Q-} \int_X \rho+(y)\psi(x,y) \, dy - \frac{Q-}{Q+ + Q-} \int_X \rho-(y)\psi(x,y) \, dy. \]

It is not difficult to check that \( \frac{\rho+(x)}{Q+} \) and \( \frac{\rho-(x)}{Q-} \) can be viewed as probability density functions because they are nonnegative over \( X \) and \( \int_X \frac{\rho+(x)}{Q+} \, dx = \int_X \frac{\rho-(x)}{Q-} \, dx = 1 \), i.e., normalized charge densities are probability density functions. Therefore, we define conditional probability density functions as

\[ p(x|+) = \frac{\rho+(x)}{Q+}, \quad p(x|-) = \frac{\rho-(x)}{Q-}, \] (2)

and prior probability as

\[ \Pr(+) = \frac{Q+}{Q+ + Q-}, \quad \Pr(-) = \frac{Q-}{Q+ + Q-}. \] (3)
Consequently, the above normalized potential function is rewritten in terms of (2) and (3) as

\[
\frac{\Phi(x)}{Q_+ + Q_-} = \Pr(+) \int_X p(y|+)\psi(x, y)dy - \Pr(-) \int_X p(y|-)\psi(x, y)dy.
\]

Hence a binary potential function classifier is defined as

\[
f(x) = \text{sign}(\Phi(x)) = \text{sign} \left( \Pr(+) \int_X p(y|+)\psi(x, y)dy - \Pr(-) \int_X p(y|-)\psi(x, y)dy \right), \tag{4}
\]

i.e., the polarity of the potential determines the class label.

2.2. PFRs and Bayes Classifiers

Next, we present a Bayesian interpretation of the above potential function classifier. In particular, we show that with a proper choice of \(\psi\), the decision boundary of (4) is identical to that of the optimal Bayes classifier. Our first choice of \(\psi\) is the Dirac delta function which is zero everywhere except at the origin, where it is infinite,

\[
\delta(x) = \begin{cases} 
+\infty & x = 0 \\
0 & x \neq 0
\end{cases}
\]

and which also satisfies the identity

\[
\int_{-\infty}^{\infty} \delta(x)dx = 1.
\]

**Theorem 1.** Let \(\rho_+\) and \(\rho_-\) be the charge densities; \(p(x|+), p(x|-), \Pr(+)\), and \(\Pr(-)\) be defined by (2) and (3). If we choose \(\psi(x, y) = \delta(x - y)\), the decision boundary of the potential function classifier (4) is equivalent to that of the Bayes classifier for conditional probability distributions \(p(x|+)\) and \(p(x|-)\), and class prior probabilities \(\Pr(+)\) and \(\Pr(-)\).

A proof of Theorem 1 is given in the Appendix. We may interpret the above theorem from the perspective of Fourier analysis. Specifically, for a translation invariant point potential function, i.e., \(\psi(x, y) = \psi(x - y)\), the evaluation of \(\int_X p(y|+)\psi(x - y)dy\) is essentially the convolution of \(p(x|+)\) and \(\psi(x)\), which is equivalent to computing the inverse Fourier transform of
the product of the Fourier transforms of \( p(x|+) \) and \( \psi(x) \). When \( \psi \) is the Dirac delta function, potential function classifiers are equivalent to Bayes classifiers because the Fourier transform of the Dirac delta function is the constant 1.

Theorem 1 holds independent of the specific forms of the charge densities, i.e., it is distribution free. Nevertheless, the unboundedness of the Dirac delta function makes it a poor choice in numerical implementations. Next, by assuming that the Fourier transform of the charge densities have finite support, we extend the conclusion of Theorem 1 to a wider class of translation invariant point potential functions.

**Theorem 2.** Let \( \rho_+ \) and \( \rho_- \) be the charge densities; \( p(x|+) \), \( p(x|-) \), \( \Pr(+) \), and \( \Pr(-) \) be defined by (2) and (3). Let \( \hat{p}_+(\omega) \) and \( \hat{p}_-(\omega) \) be the Fourier transform of \( p(x|+) \) and \( p(x|-) \), respectively, i.e.,

\[
\hat{p}_+(\omega) = \int_X p(x|+) e^{-2\pi i \omega^T x} dx,
\]
\[
\hat{p}_-(\omega) = \int_X p(x|-) e^{-2\pi i \omega^T x} dx,
\]

where \( i \) is the complex number \( \sqrt{-1} \). We assume that \( \hat{p}_+ \) and \( \hat{p}_- \) have finite support, namely, there exist constants \( s_+ \) and \( s_- \) such that \( \hat{p}_+(\omega) = 0 \) for \( \|\omega\| \geq s_+ \) and \( \hat{p}_-(\omega) = 0 \) for \( \|\omega\| \geq s_- \). For any translation invariant point potential function \( \psi(x,y) = \psi(x-y) \), if its Fourier transform satisfies that \( \Psi(\omega) = 1 \) for \( \|\omega\| < s = \max(s_+, s_-) \), the decision boundary of the potential function classifier (4) is identical to that of the Bayes classifier using conditional probability distributions \( p(x|+) \) and \( p(x|-) \), and class prior probabilities \( \Pr(+) \) and \( \Pr(-) \).

A proof of Theorem 2 is given in the Appendix. The above theorem states that if the charge densities are ‘band limited’ (i.e., its Fourier transform is zero everywhere outside a hyperball of finite radius \( s \)) and the point potential function has value 1 over the support of charge densities in the frequency domain, the potential function conveys the same information as the class conditional density. In the one dimensional case, a possible choice of \( \psi \) is a sinc function,

\[
\psi(x, y) = \frac{\sin[2\pi s(x - y)]}{\pi(x - y)} = 2s \cdot \text{sinc}[2s(x - y)],
\]
whose Fourier transform is a rectangular window function
\[
\Psi(\omega) = \begin{cases} 
1 & |\omega| \leq s \\
0 & |\omega| > s
\end{cases} = \text{rect} \left( \frac{\omega}{2s} \right). 
\]

This choice of \(\Psi\) can be generalized to higher dimensional spaces: for a hyper-rectangular window function in a \(d\)-dimensional frequency domain,
\[
\Psi(\omega) = \begin{cases} 
1 & |\omega_i| \leq s, \forall i \in [1,d] \\
0 & |\omega_i| > s, \exists i \in [1,d]
\end{cases} = \prod_{i=1}^{d} \text{rect} \left( \frac{\omega_i}{2s} \right),
\]

the corresponding point potential function is
\[
\psi(x, y) = (2s)^d \prod_{i=1}^{d} \text{sinc}[2s(x_i - y_i)]. 
\] (5)

Theorem 2 has implications on the practical design of potential function classifiers using a finite training set. This will be discussed in the next section.

In statistics, an idea similar to Theorem 2 had been explored in nonparametric density estimation. Watson and Leadbetter [68] discussed the \(L_2\) error of kernel density estimates and related it to the spectral property of the density function (i.e., characteristic function). They concluded that the form of the optimal estimate depends critically on the tail of the characteristic function. Davis [23, 24] showed that using a sinc kernel, with a carefully chosen scale factor, the Fourier integral error estimate is asymptotically optimal within a constant factor for all densities. The analyses in [68, 23, 24] were performed under the \(L_2\) measure. Devroye [27, 28, 29] developed a series of asymptotic performance bounds for kernel estimates using the \(L_1\) measure. Compared with the \(L_2\) error, the \(L_1\) error has a clearer physical interpretation. As consistent density estimates yield consistent classifiers, a plug-in decision rule using these kernel density estimates is naturally consistent.

### 3. Potential Function Rules as Plug-in Decision Rules

The main difficulty of using the potential function classifier (4) is that charge densities are usually unknown. An approximation method is therefore presented in this section. Next, we first generalize the above binary potential function classifier to multiple classes. All the results discussed in Section 2 can be extended to the multi-class scenario. We then present an approximation on PFR and a discussion on its connection with plug-in decision rules.
3.1. An Approximation on Multi-class Potential Function classifiers

Let \( z \in \mathbb{K} = \{1, \ldots, K\} \) be the class label of observation \( x \in X \). The observation-label pair \((x, z)\) is generated by a distribution \( F \), which is a mixture of \( K \) unknown distributions \( F_1, \ldots, F_K \),

\[
F = \sum_{k=1}^{K} P_k F_k,
\]

where \( P_k \) is the marginal probability of label \( k \), i.e., \( P_k = \Pr(z = k) \); \( F_k \) is the cumulative distribution function of \( x \) conditioned on \( z = k \). Analogous to (1), (2), and (3), we define \( \Phi_k \) as a class potential function - the potential with respect to \( P_k F_k \):

\[
\Phi_k(x) = P_k \int_X \psi(x, y) dF_k(y) .
\]

A multi-class potential classifier is defined as

\[
f(x) = \arg\max_k \Phi_k(x) .
\]

Note that the class potential (6) is the product of \( P_k \) and the expectation of the point potential function \( \psi \) with respect to \( F_k \), i.e.,

\[
\Phi_k(x) = P_k \mathbb{E}_{y \sim F_k} [\psi(x, y)] .
\]

Although \( F \) is unknown in most applications, a training set is usually given. Therefore, we approximate the above expectation by the sample mean. Let \( S = \{(x_1, z_1), \ldots, (x_\ell, z_\ell)\} \subset X \times \mathbb{K} \) be the training set, a random i.i.d. sample from \( F \).

**Definition 1 (Sample Class Potential Function).** Given a point potential function \( \psi : X \times X \to \mathbb{R} \), we define the sample class potential of an observation \( x \) with respect to class \( k \) and sample \( S \) as

\[
\phi_k(x, S) = \frac{1}{|S|} \sum_{z_i = k} \psi(x, x_i) .
\]

A multi-class sample potential classifier is then defined using sample class potential functions as follows.
Definition 2 (A Multi-class Sample Potential Function Classifier). Given $S$, a set of i.i.d. training samples generated by an unknown distribution $F$ on $\mathbb{X} \times \mathbb{K}$, we define a potential classifier $f_S : \mathbb{X} \to \mathbb{K}$ as

$$f_S(x) = \arg\max_k \phi_k(x, S). \quad (9)$$

Clearly, the sample class potential (8) can be written as

$$\phi_k(x, S) = \frac{|S_k|}{|S|} \sum_{z_i = k} \psi(x, x_i),$$

where $S_k = \{(x, z) \in S : z = k\}$. It is not difficult to observe that $\frac{|S_k|}{|S|}$ is an estimate of the marginal probability $P_k$. Furthermore, if we restrict $\psi$ to be a nonnegative translation invariant function and $\int_{\mathbb{X}} \psi(x)dx = c < \infty$, it is straightforward to show that $\frac{1}{c|S|} \sum_{z_i = k} \psi(x, x_i)$ is an estimate of the probability density of $F_k$ at location $x$ using the kernel density estimation ($\psi$ is the kernel function). Hence, for any given $x$, $\phi_k(x, S)$ is proportional to an estimation of the posterior probability $Pr(z = k|x)$.

This implies that the family of multi-class potential function classifiers (9) includes those plug-in decision Bayes classifiers that use kernel density estimation. Therefore, if $\psi$ is chosen from regular kernels, the universal consistency of PFRs follows from the universal consistency of kernel rules (Devroye et al. [30]). Universal consistency characterizes an asymptotic property of a decision rule - a decision rule converges to the optimal solution as the number of training sample is sufficiently large. For kernel rules, universal consistency requires the ‘width’ of the kernel to decrease to 0 as the sample size increases to infinity. Next, we show that under the conditions of Theorem 2, for a fixed width of $\psi$ (i.e., $\frac{1}{s}$ in (5) is fixed), with high probability the prediction of a sample PFR converges to that of the Bayes classifier for any given input.

It is worth noting that when the point potential function $\frac{1}{\|x-y\|}$ is used, the above PFR is called Hilbert rule. Hilbert rules were investigated by Devroye, Krzyżak, and Györfi for density estimation, regression and classification [31, 32, 33]. An interesting property of Hilbert rules is that it does not have a smoothing parameter. Consistency theory of Hilbert rules was developed in [31, 32, 33].

3.2. The Potential Gap and the Generalization Performance

For a set of numbers $a_1, \ldots, a_K$, the $k$-th smallest number is denoted by $a_{(k)}$, i.e., $a_{(1)} \leq a_{(2)} \leq \cdots \leq a_{(K)}$. We define the potential gap of a multi-class
classifier $f$ given in (7) on an observation $x$ by

$$\Gamma(x) = \Phi_{f(x)}(x) - \Phi_{(K-1)}(x),$$

which is the difference between the largest class potential and the second largest class potential at $x$. It should be clear that $\Gamma(x) \geq 0$. The following theorem demonstrates that under the conditions of Theorem 2 (class conditional densities are band limited), the performance of a sample potential classifier (9) is closely related to the potential gap.

**Theorem 3.** Let $S = \{(x_1, z_1), \ldots, (x_\ell, z_\ell)\} \subset \mathbb{R}^d \times \mathbb{K}$ be a random i.i.d. sample from $F$, a mixture of $K$ distributions $F_1, \ldots, F_K$: $F = \sum_{k=1}^{K} P_k F_k$, where $P_k$ is the marginal probability of class $k$; $F_k$, defined by a density function $p_k(x)$, is the distribution of $x$ for class $k$. The conditional density functions are band limited, i.e., there exists $s > 0$ such that $\hat{p}_k(\omega) = 0$ when $||\omega|| \geq s$ for all $k = 1, \ldots, K$, where $\hat{p}_k(\omega)$ is the Fourier transform of $p_k(x)$. For any $x \in \mathbb{R}^d$ the following inequality holds:

$$\Pr[f_S(x) \neq f^*(x)] \leq 2Ke^{\frac{\ell \Gamma(x)^2}{2(2s)^2d}},$$

where $f_S(x)$ is the sample potential function classifier given in Definition 2 with (5) being the point potential function, $f^*(x)$ the Bayes classifier, and $\Gamma(x)$ the potential gap.

A proof of Theorem 3 is given in the Appendix.

Theorem 3 suggests that for any given $x$ and a band limited joint probability density function, the probability that the sample potential function classifier behaves differently from the Bayes classifier depends on two parameters: the potential gap $\Gamma(x)$ and the sample size $\ell$. The larger the potential gap and the sample size, the more likely that the sample potential function classifier makes the optimal prediction. In this sense, the generalization performance of $f_S$ depends on the potential gap. Nevertheless, Theorem 3 does not tell us how to pick a sample size $\ell$, neither could we compute the right hand side of the inequality (11), because the potential gap is unknown in practice. Motivated by the potential gap, we present, in the next section, a probabilistic bound on the generalization performance of a sample potential function classifier based on the margin of $f_S$, which is closely related to the sample version of the potential gap.
4. A Generalization Bound for Potential Function Classifiers

As indicated in Definition 1, the sample class potential \( \phi_k(x, S) \) is an estimate of the class potential \( \Phi_k(x) \). Analogous to the potential gap, we define the margin of \( f_S \) on an observation \( (x, z) \in \mathbb{R}^d \times \mathbb{K} \) as

\[
\gamma(x, z, S) = \phi_2(x, S) - \phi_{(K-1)}(x, S).
\] (12)

Given a classifier \( f_S \) and a desired margin \( \alpha > 0 \), we denote by \( \xi \) the bounded amount by which \( f_S \) fails to achieve the desired margin \( \alpha \) on sample \( (x, z) \),

\[
\xi = \min\{\alpha, [\alpha - \gamma(x, z, S)]_+\},
\]

where \([x]_+ = x \) if \( x \geq 0 \) and 0 otherwise. For an observation \( (x_i, z_i) \in S \), we define its margin shortage, \( \xi_i \), as

\[
\xi_i = \min\{\alpha, [\alpha - \gamma(x_i, z_i, S(i))]_+\},
\] (13)

where \( S(i) = S - \{(x_i, z_i)\} \). Note that both \( \xi \) and \( \xi_i \in [0, \alpha] \).

We illustrate the concepts of margin and \( \xi \) in Figure 1 under a 3-class scenario. The solid curve in Figure 1(a) shows the variations of the margin for an observation, \( (x, 3) \), as a function of its sample class potential \( \phi_3(x, S) \). The sample class potentials of \( x \) with respect to class 1 and class 2, i.e, \( \phi_1(x, S) \) and \( \phi_2(x, S) \), are fixed. For a desired margin \( \alpha = 0.3 \), the dashed curve represents the value of \( \xi \): the bounded amount by which the margin is less than \( \alpha \). Figure 1(b) shows three sample class potential functions constructed from 12 training observations. Each class is associated with a distinct marker: circle, triangle, or square. The point potential function defined in (5) with \( s = 0.1 \) is used in the evaluation of the sample class potential functions. We visualize the margin for each training observation using an arrow where the margin is computed as the difference between the vertical coordinate of the tip of the arrow \( (\phi_2(x, S)) \) and that of the end of the arrow \( (\phi_2(x, S)) \). The numerical value of a margin is also listed along with the arrow. For observations \( (-0.5, 2) \) and \( (4, 3) \), the arrows are absent because their margins are 0.

It is not difficult to relate margins to classification errors. Positive margins suggest correct classifications. Negative margins imply mis-classifications. There are only two scenarios that result in the 0 margin: \( \phi_2(x, S) = \phi_{(K)}(x, S) = \phi_{(K-1)}(x, S) \) or \( \phi_{(K)}(x, S) > \phi_2(x, S) = \phi_{(K-1)}(x, S) \). In the former case, which is rare in practice, the correctness of the classification depends on the
Figure 1: Sample class potential functions and margins under a 3-class scenario. (a) The solid curve describes the variation of margin $\gamma(x, 3, \mathcal{S})$ with respect to the sample class potential $\phi_3(x, \mathcal{S})$ when the sample class potential $\phi_1(x, \mathcal{S})$ and $\phi_2(x, \mathcal{S})$ are fixed. The dashed curve represents $\xi$, the bounded amount by which the margin is less than $\alpha = 0.3$. (b) The three curves represent sample class potential functions built upon 12 training observations (denoted by the markers on the horizontal axis) using a 1-d sinc point potential function with $s = 0.1$. Each arrow corresponds to a margin, which is computed as the difference between the vertical coordinate of the tip of the arrow and that of the end of the arrow. The numeric value of the margin is given along with the arrow. The arrow is absent if the margin is 0.
tie breaking strategy, which is usually random. The second case is more common, for example the two 0 margins in Figure 1(b). It leads to mis-classifications. If we introduce the following indicator function

\[ I(x, z, S) = \begin{cases} 
1 & \gamma(x, z, S) \leq 0 \\
0 & \text{otherwise} 
\end{cases} \]

(14)

\[ \sum_{i=1}^{\ell} I(x_i, z_i, S(i)) \] is an upper bound on the number of mis-classified observations in a leave-one-out evaluation.

The connection between the bounded margin shortage \( \xi_i \), which is defined in (13), and a classification error is more subtle. If we divide \( \xi_i \) by \( \alpha \), we have

\[ \frac{\xi_i}{\alpha} = \begin{cases} 
1 & \gamma(x_i, z_i, S(i)) \leq 0 \\
1 - \frac{\gamma(x_i, z_i, S(i))}{\alpha} & 0 < \gamma(x_i, z_i, S(i)) \leq \alpha \\
0 & 0 < \gamma(x_i, z_i, S(i)) \leq \alpha 
\end{cases} \]

(15)

Figure 2(a) compares \( \frac{\xi_i}{\alpha} \) with \( I(x_i, z_i, S(i)) \) as a function of \( \gamma(x_i, z_i, S(i)) \). It is clear that \( \frac{\xi_i}{\alpha} \) is always greater than or equal to \( I(x_i, z_i, S(i)) \). Therefore, \( \sum_{i=1}^{\ell} \frac{\xi_i}{\alpha} \) is an upper bound on the number of mis-classified observations in a leave-one-out evaluation. Next, we present a generalization bound based on the desired margin \( \alpha \) and the bounded margin shortage \( \xi_i \) for any given
bounded point potential function \( \psi \). Without loss of generality, we assume that \( \psi : X \times X \to [0, 1] \).

**Theorem 4.** Let \( S = \{(x_1, z_1), \ldots, (x_\ell, z_\ell)\} \subset X \times K \) be a random i.i.d. sample from an unknown distribution \( F \), and \( f_S : X \to K \) a sample potential function classifier defined according to (9) using a given point potential function \( \psi : X \times X \to [0, 1] \). For a fixed \( \delta \in (0, 1) \), a desired margin \( \alpha > 0 \), and a new random sample \((x, z)\) generated from \( F \), the following bound holds with probability at least \( 1 - \delta \) over \( S \):

\[
\Pr_F[z \neq f_S(x)|S] \leq \frac{1}{\ell} \sum_{i=1}^{\ell} \frac{\xi_i}{\alpha} + \frac{2}{\ell \alpha} + \left(1 + \frac{4}{\alpha}\right) \sqrt{\frac{\ln(2/\delta)}{2\ell}}. \tag{16}
\]

where \( \xi_i \) is defined in (13).

A proof of Theorem 4 is given in the Appendix. It is worthwhile to note that there are two sources of randomness in the above inequality: the random sample \( S \) and the random observation \((x, z)\). For a specific \( S \), the above bound is either true of false, i.e., it is not random. For a random sample \( S \), the probability that the bound is true is at least \( 1 - \delta \). The inequality shows that the error probability, \( \Pr_F[z \neq f_S(x)|S] \), of a sample potential function classifier depends on three terms. The first term, \( \frac{1}{\ell} \sum_{i=1}^{\ell} \frac{\xi_i}{\alpha} \), is an upper bound on the leave-one-out training error. The second and the third terms are determined by the training sample size \( \ell \), the desired margin \( \alpha \), and the confidence parameter \( \delta \). In general, for fixed \( \ell \) and \( \delta \), the generalization performance of \( f_S \) is a trade-off between training error and the desired margin \( \alpha \). On one hand, a smaller \( \alpha \) produces a tighter bound on the training error, but larger values for the second and the third term. On the other hand, a larger \( \alpha \) can reduce the values of the second and the third term, but makes the first term a looser bound on the training error. This is illustrated in Figure 2(b) using margins generated from a uniform distribution on \([-0.1, 1]\). The values of the upper bound are shown as a function of the desired margin \( \alpha \). In the next section, we discuss classifier selection methods motivated by the above bound on the generalization performance.

5. Margin Distributions and Classifier Selection

The learning of a potential function classifier is essentially the selection of a point potential function (or its parameters). Figure 2(b) shows that
given $\ell$ and $\delta$, the upper bound on the probability of error has a minimum. Hence it is tempting to choose a classifier that minimizes the upper bound in (16). Unfortunately, this is not an effective approach in practice because the bound is usually loose even for large training sets with $50,000–100,000$ observations.

As we discussed in Section 4, the desired margin $\alpha$ plays a key role in estimating the generalization performance. If we define

$$i^* = \arg\min_{i=1,\ldots,\ell} \gamma(x_i, z_i, S(i)),$$

it is clear from Figure 2(a) that $\frac{1}{\ell} \sum_{i=1}^{\ell} \frac{\xi_i}{\alpha}$ achieves the minimum (which is equal to the training error) when $0 < \alpha \leq \gamma(x_{i^*}, z_{i^*}, S(i^*))$. Although a larger value of $\alpha$ decreases the values of the last two terms in (16), it also increases the value of $\frac{1}{\ell} \sum_{i=1}^{\ell} \frac{\xi_i}{\alpha}$. However, for a fixed value of $\alpha$, the bound is tighter if the margins are concentrated more towards the positive end than towards the negative end. This suggests that we may select classifiers based on the distribution of margins.

However, a direct comparison of margin distributions may not be meaningful because the support region of a margin distribution largely depends

---

2This is because there will be no observations whose margin falls into the sloped region. Hence $\frac{1}{\ell} \sum_{i=1}^{\ell} \frac{\xi_i}{\alpha} = \frac{1}{\ell} \sum_{i=1}^{\ell} I(x_i, z_i, S(i))$, which is the leave-one-out training error.
on the selected point potential function $\psi$ and its parameters. For example, Figure 3(a) shows the probability distributions of margins under a Gaussian point potential function (i.e., $\psi(x, y) = e^{-\frac{\Vert x-y \Vert^2}{\sigma^2}}$) using the MAGIC dataset from UCI Machine Learning Repository (details of the dataset are given in Section 6). The support region of the margin distribution varies significantly with the values of $\sigma$.

To make margins comparable under different point potential functions or different parameter values, we propose the following normalization procedure. For any given $x \in \mathbb{R}^d$, we define a normalized sample class potential, $\hat{\phi}_k(x, S)$, as

$$\hat{\phi}_k(x, S) = \frac{\phi_k(x, S)}{\sum_{i=1}^K |\phi_i(x, S)|}.$$ 

Clearly, the above normalization does not change the order of sample class potentials, hence the classification decisions. The normalized margin of $f_S$ on an observation $(x, z) \in \mathbb{R}^d \times \mathbb{K}$ is then defined as

$$\hat{\gamma}(x, z, S) = \hat{\phi}_z(x, S) - \hat{\phi}_{(K-1)}(x, S).$$

Figure 3(b) shows the probability densities of the margins after normalization. In both figures, the densities are shown under a log transformation. As we discussed in Section 3.1, if $\psi$ is a nonnegative translation invariant function that is integrable over $\mathbb{X}$, $\phi_k(x, S)$ is proportional to an estimation of the posterior probability $\Pr(z = k|x)$. The normalized class potential, $\hat{\phi}_k(x, S)$, is an estimate of the posterior probability $\Pr(z = k|x)$. Hence the normalized margin $\hat{\gamma}$ can be viewed as an estimation on the posterior probability gap.

In classifier selection, we would like to choose a classifier whose margins concentrate towards the positive end. In terms of normalized margin, this suggests that $\hat{\gamma}$ should concentrate towards 1. We propose the following metric:

$$h(f_S) = \text{var}_{\hat{\gamma}} - \text{mean}_{\hat{\gamma}}$$

where $\text{mean}_{\hat{\gamma}} = \frac{1}{L} \sum_{i=1}^L \hat{\gamma}(x_i, z_i, S(i))$ and $\text{var}_{\hat{\gamma}} = \frac{1}{L-1} \sum_{i=1}^L [\hat{\gamma}(x_i, z_i, S(i)) - \text{mean}_{\hat{\gamma}}]^2$. Clearly, the desired normalized margins should have large mean and small variance, i.e., we select a classifier that minimizes $h$.

6. Experimental Results

We compare the proposed model selection method using normalized margin distribution with a traditional approach using the leave-one-out training
Table 1: The comparison results of model selection using leave-one-out error and the margin distribution metric defined in (17). \( \ell_{\text{train}} \): the size of training set; \( \ell_{\text{test}} \): the size of test set; \( d \): feature dimension; \( K \): the number of classes; \( n_B \): the number of experiments in which the proposed method performs better than leave-one-out model selection; \( n_E \): the number of experiments in which the proposed method and leave-one-out model selection have same test error; \( n_W \): the number of experiments in which the proposed method performs worse than leave-one-out model selection.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>( \ell_{\text{train}} )</th>
<th>( \ell_{\text{test}} )</th>
<th>( d )</th>
<th>( K )</th>
<th>( n_B )</th>
<th>( n_E )</th>
<th>( n_W )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balancescale</td>
<td>570</td>
<td>55</td>
<td>4</td>
<td>2</td>
<td>7</td>
<td>37</td>
<td>6</td>
</tr>
<tr>
<td>Bloodtransfusion</td>
<td>600</td>
<td>148</td>
<td>4</td>
<td>2</td>
<td>29</td>
<td>13</td>
<td>8</td>
</tr>
<tr>
<td>Breastcancer</td>
<td>600</td>
<td>83</td>
<td>9</td>
<td>2</td>
<td>10</td>
<td>39</td>
<td>1</td>
</tr>
<tr>
<td>Ecoli</td>
<td>200</td>
<td>136</td>
<td>7</td>
<td>8</td>
<td>15</td>
<td>22</td>
<td>13</td>
</tr>
<tr>
<td>Glass</td>
<td>150</td>
<td>64</td>
<td>9</td>
<td>6</td>
<td>22</td>
<td>21</td>
<td>7</td>
</tr>
<tr>
<td>Imageseg</td>
<td>2100</td>
<td>210</td>
<td>19</td>
<td>7</td>
<td>15</td>
<td>22</td>
<td>13</td>
</tr>
<tr>
<td>Ionosphere</td>
<td>320</td>
<td>31</td>
<td>34</td>
<td>2</td>
<td>5</td>
<td>29</td>
<td>16</td>
</tr>
<tr>
<td>Letter</td>
<td>18000</td>
<td>2000</td>
<td>16</td>
<td>26</td>
<td>32</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>Liver</td>
<td>300</td>
<td>45</td>
<td>6</td>
<td>2</td>
<td>23</td>
<td>14</td>
<td>13</td>
</tr>
<tr>
<td>Magic</td>
<td>10000</td>
<td>9020</td>
<td>10</td>
<td>2</td>
<td>44</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Multi-Feature1</td>
<td>1800</td>
<td>200</td>
<td>216</td>
<td>10</td>
<td>9</td>
<td>34</td>
<td>7</td>
</tr>
<tr>
<td>Multi-Feature2</td>
<td>1800</td>
<td>200</td>
<td>64</td>
<td>10</td>
<td>7</td>
<td>43</td>
<td>0</td>
</tr>
<tr>
<td>Multi-Feature3</td>
<td>1800</td>
<td>200</td>
<td>240</td>
<td>10</td>
<td>9</td>
<td>39</td>
<td>2</td>
</tr>
<tr>
<td>Satimage</td>
<td>5835</td>
<td>600</td>
<td>36</td>
<td>6</td>
<td>16</td>
<td>23</td>
<td>11</td>
</tr>
<tr>
<td>Sonar</td>
<td>150</td>
<td>58</td>
<td>60</td>
<td>2</td>
<td>15</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td>Spectfheart</td>
<td>200</td>
<td>67</td>
<td>44</td>
<td>2</td>
<td>3</td>
<td>37</td>
<td>0</td>
</tr>
<tr>
<td>Survival</td>
<td>206</td>
<td>100</td>
<td>3</td>
<td>2</td>
<td>22</td>
<td>8</td>
<td>20</td>
</tr>
<tr>
<td>Vehicle</td>
<td>800</td>
<td>46</td>
<td>18</td>
<td>4</td>
<td>8</td>
<td>31</td>
<td>11</td>
</tr>
<tr>
<td>Vowel</td>
<td>890</td>
<td>100</td>
<td>10</td>
<td>11</td>
<td>3</td>
<td>33</td>
<td>14</td>
</tr>
<tr>
<td>Winequality</td>
<td>6000</td>
<td>497</td>
<td>11</td>
<td>7</td>
<td>17</td>
<td>0</td>
<td>33</td>
</tr>
</tbody>
</table>

error. The experiments were conducted on 20 datasets from UCI Machine Learning Repository. Each dataset is randomly divided into a training set and a test set. We built a potential function classifier with Gaussian point potential function for each dataset. The bandwidth parameter \( \sigma \) of the point potential function is determined from 20 different values (0.03, 0.04, 0.05, 0.06, 0.07, 0.08, 0.09, 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0, 2.0, 3.0, and 4.0), using two strategies: (1) minimizing the leave-one-out training error; (2) minimizing the margin distribution metric defined in (17). The above procedure was repeated for 50 runs. In each run, test errors were recorded. In Table 1, we list the names of the datasets, the sizes of training and test sets, the dimension of the feature space, the number of categories, and the number of runs in which the proposed model selection method outperformed
(n_B), tied with (n_E), and underperformed (n_W) the leave-one-out approach. Among the 20 datasets, the proposed method outperformed the leave-one-out model selection on 15 datasets (i.e. n_B > n_W), which are highlighted in Table 1. The two approaches tied on 1 dataset (Sonar). This suggests a very competitive performance of the proposed method.

7. Conclusions

In this paper, we revisited potential function rules (PFRs) in their original form and reveal their connections with other well-known results in the literature. We derive a bound on the generalization performance of potential function classifiers based on the observed margin distribution of the training data. A new model selection criterion using a normalized margin distribution is then proposed to learn “good” potential function classifiers in practice. We evaluated the proposed model selection method over 20 UCI data sets. In comparison with the traditional model selection using leave-one-out training error, the margin distribution based metric demonstrates very competitive performance.

Acknowledgments

This work was supported by the US National Science Foundation under award number MCB-1027989 and EPS-0903787.

Appendix A.

Proof of Theorem 1: Because δ(·) is a Dirac delta function, it follows that

\[ \int_X p(y|+)dx \delta(x - y)dy = p(x|+), \int_X p(y|-)dx \delta(x - y)dy = p(x|-). \]

Therefore,

\[ \Pr(+) \int_X p(y|+)dx \delta(x - y)dy \propto \Pr(+|x) \]

\[ \Pr(-) \int_X p(y|-)dx \delta(x - y)dy \propto \Pr(-|x), \]

i.e., the potential of the positive (negative) class is proportional to the posterior probability of the positive (negative) class. Hence the decision boundary of (4) is identical to that of the Bayes classifier. □
Proof of Theorem 2: For a translation invariant $\psi$,
\[
\int_X p(y|+\psi(x, y)dy = \int_X p(y|+\psi(x - y)dy = \mathcal{F}^{-1}[\hat{p}_+(\omega)\Psi(\omega)]
\]
where $\mathcal{F}^{-1}$ is the inverse Fourier transform. Because $\hat{p}_+(\omega) = 0$ for $||\omega|| \geq s$ and $\Psi(\omega) = 1$ for $||\omega|| \leq s$, we have $\hat{p}_+(\omega)\Psi(\omega) = \hat{p}_+(\omega)$. It follows that
\[
\Pr(+\int_X p(y|+\psi(x, y)dy = \Pr(+|p(x|+) \propto \Pr(+|x).
\]
Similarly,
\[
\Pr(-\int_X p(y|-\psi(x, y)dy = \Pr(-|p(x|-) \propto \Pr(-|x).
\]
The potential of the positive (negative) class hence is proportional to the posterior probability of the positive (negative) class. Therefore the decision boundary of (4) is identical to that of the Bayes classifier.

We need the following Lemma to prove Theorem 3.

Lemma 1. For any $a_1, a_2, \ldots, a_K \in \mathbb{R}$ and $b_1, b_2, \ldots, b_K \in \mathbb{R}$, if $|a_k - b_k| \leq \epsilon$ for all $k \in \mathbb{K}$, we have $|a_{(j)} - b_{(j)}| \leq \epsilon$ for all $j \in \mathbb{K}$.

Proof: For any $j \in \mathbb{K}$,
\[
a_{(j)} - \epsilon \leq a_{(j+1)} - \epsilon \leq \cdots \leq a_{(K)} - \epsilon.
\]
Because $b_k \geq a_k - \epsilon$ for all $k \in \mathbb{K}$, the number of $b_k$’s that are greater than or equal to $a_{(j)} - \epsilon$ is at least $K - j + 1$. Therefore $b_{(j)} \geq a_{(j)} - \epsilon$. Similarly, for any $j \in \mathbb{K}$,
\[
a_{(1)} + \epsilon \leq a_{(2)} + \epsilon \leq \cdots \leq a_{(j)} + \epsilon.
\]
Because $b_k \leq a_k + \epsilon$ for all $k \in \mathbb{K}$, the number of $b_k$’s that are less than or equal to $a_{(j)} + \epsilon$ is at least $j$. Therefore $b_{(j)} \leq a_{(j)} + \epsilon$. This completes the proof.

Proof of Theorem 3: We introduce a new random variable $S_k = |\{(x, z) \in \mathcal{S} : z = k\}|$. For any given $x$,
\[
E_{p}[\phi_k(x, S)] = \mathbb{E}_{S_k} \left\{ \mathbb{E}_{F|S_k} \left[ \frac{S_k}{\ell} \frac{1}{S_k} \sum_{z_i = k} \psi(x, x_i) \right] \right\} = \mathbb{E}_{S_k} \left\{ \frac{S_k}{\ell} \mathbb{E}_{y \sim F_k} [\psi(x, y)] \right\} = P_k \mathbb{E}_{y \sim F_k} [\psi(x, y)] = \Phi_k(x).
\]
We rewrite $\phi_k(x, S)$ as $\phi_k(x, S) = \frac{1}{\ell} \sum_{i=1}^{\ell} I(z_i = k)\psi(x, x_i)$ where the indicator function $I(z_i = k) = 1$ if $z_i = k$, $I(z_i = k) = 0$ otherwise. Because $(x_i, z_i)$’s are i.i.d., so are $I(z_i = k)\psi(x, x_i)$. In addition, from (5) it is clear that $|I(z_i = k)\psi(x, x_i)| \leq (2s)^d$ . It follows from Hoeffding’s inequality that for any given $x$, $\epsilon > 0$, and $k = 1, \ldots, K$,
\[
\Pr[|\phi_k(x, S) - \Phi_k(x)| \geq \epsilon] \leq 2e^{-\frac{2\epsilon^2}{(2s)^d}} . \tag{A.1}
\]
Because the conditional densities are band limited, it follows from the proof of Theorem 2 that
\[ \Phi_k(x) = P_k E_{\mathcal{Y}, \mathcal{P}_k}[\psi(x, y)] \propto P(z = k|x) . \]
Hence we have \[ f^*(x) = \arg\max_k \Phi_k(x) . \] From Lemma 1, we know that \[ |\phi_k(x, S) - \Phi_k(x)| \leq \frac{\Gamma(x)}{2} \] for \( k = 1, \ldots, K, \) \[ |\phi_{(k)}(x, S) - \Phi_{(k)}(x)| \leq \frac{\Gamma(x)}{2} . \] Combining this with the facts that
\[ \phi_{f_S(x), S} = \phi_{(k)}(x, S) \] and \[ \Phi_{f^*(x)}(x) = \Phi(k)(x) , \]
it is straightforward to derive that \( f_S(x) = f^*(x) . \) Therefore,
\[ \text{Pr} \left[ |\phi_k(x, S) - \Phi_k(x)| < \frac{\Gamma(x)}{2}, \; \forall \; k = 1, \ldots, K \right] \leq \text{Pr}[f_S(x) = f^*(x)] . \quad (A.2) \]
Let \( \epsilon = \frac{\Gamma(x)}{2} . \) Using (A.1), (A.2), and the union bound, we have
\[ \text{Pr} [f_S(x) \neq f^*(x)] \leq \text{Pr} \left[ \exists k, \; |\phi_k(x, S) - \Phi_k(x)| \geq \frac{\Gamma(x)}{2} \right] \leq 2K e^{-\frac{\epsilon^2(x)}{2\ell+1}} . \]
This completes the proof. \( \Box \)

In order to prove the upper bound on generalization of sample potential function classifiers in Theorem 4, we need the following Lemma and an inequality attributed to McDiarmid.

**Lemma 2.** Let \( S(i) = S - \{ (x_i, z_i) \} . \) For a change of one \( (x_t, z_t) \) to \( (x_t, \hat{z}_t) , \) denote
\[ \hat{S}_i = \{ (x_1, z_1), \ldots, (x_{t-1}, z_{t-1}), (x_t, \hat{z}_t), (x_{t+1}, z_{t+1}), \ldots, (x_t, z_t) \} . \]
We define \( \hat{S}_i(i) = \hat{S}_i - \{ (x_i, z_i) \} , \) hence \( \hat{S}_i(t) = S(t) . \) Let \( x \in X \) be any observation in \( X \) and \( z \in \mathbb{K} \) a class label. The following inequalities hold for any point potential function \( \psi : X \times X \to [0, 1] : \)
\[ |\gamma(x, z, S) - \gamma(x, z, S(i))| \leq \frac{2}{\ell} , \quad (A.3) \]
\[ |\gamma(x, z, S(i)) - \gamma(x, z, \hat{S}_i(i))| \leq \frac{2}{\ell-1} , \quad (A.4) \]
\[ |\gamma(x_i, z_i, S(i)) - \gamma(x_i, z_i, \hat{S}_i(i))| \leq \frac{2}{\ell-1} , \; \text{if} \; i \neq t . \quad (A.5) \]

**Proof:** It is readily checked that for any \( z \in \mathbb{K} , \)
\[ |\phi_z(x, S) - \phi_z(x, S(i))| = \left\{ \begin{array}{ll} \frac{1}{\ell} \sum_{j=z} \psi(x, x_j) & \text{if} \; z = z_i \\ \frac{1}{\ell} \sum_{j=z} \psi(x, x_j) - \frac{1}{\ell-1} \sum_{j=z, j \neq i} \psi(x, x_j) & \text{if} \; z \neq z_i \end{array} \right. \]
\[ = \left\{ \begin{array}{ll} \frac{1}{\ell} \psi(x, x_i) - \frac{1}{\ell-1} \sum_{j=z, j \neq i} \psi(x, x_j) & \leq \frac{1}{\ell} \text{if} \; z = z_i \\ \frac{1}{\ell-1} \sum_{j=z} \psi(x, x_j) & \leq \frac{1}{\ell} \text{if} \; z \neq z_i \end{array} \right. . \]
From (12) we have
\[ |\gamma(x, z, S) - \gamma(x, z, S(i))| = |\phi_z(x, S) - \phi_{(K-1)}(x, S) - \phi_z(x, S(i)) + \phi_{(K-1)}(x, S(i))| \]
\[ \leq \frac{1}{\ell} + |\phi_{(K-1)}(x, S) - \phi_{(K-1)}(x, S(i))| \leq \frac{2}{\ell}, \]
where the last step is based on Lemma 1.

It is not difficult to show that for any \( z \in \mathbb{K} \), \( |\phi_z(x, S(i)) - \phi_z(x, \hat{S}_t(i))| = 0 \) when \( i = t \), otherwise,
\[
|\phi_z(x, S(i)) - \phi_z(x, \hat{S}_t(i))| = \left\{ \begin{array}{ll}
0 & \text{if } z_t \neq z, \hat{z}_t \neq z \\
\frac{1}{\ell-1} \psi(x, x_t) & \text{if } z_t \neq z, \hat{z}_t = z \\
\frac{1}{\ell-1} \psi(x, \hat{x}_t) - \frac{1}{\ell-1} \psi(x, x_t) & \text{if } z_t = z, \hat{z}_t = z \\
\frac{1}{\ell-1} \psi(x, x_t) & \text{if } z_t = z, \hat{z}_t \neq z
\end{array} \right.
\]
Therefore,
\[
|\gamma(x, z, S(i)) - \gamma(x, z, \hat{S}_t(i))| \leq \frac{2}{\ell - 1}
\]
Finally, for \( i \neq t \) and any \( z_i \in \mathbb{K} \),
\[
|\phi_{z_i}(x_i, S(i)) - \phi_{z_i}(x_i, \hat{S}_t(i))| = \left\{ \begin{array}{ll}
0 & \text{if } z_t \neq z_i, \hat{z}_t \neq z_i \\
\frac{1}{\ell-1} \psi(x_i, x_t) & \text{if } z_t \neq z_i, \hat{z}_t = z_i \\
\frac{1}{\ell-1} \psi(x_i, x_t) - \frac{1}{\ell-1} \psi(x_i, \hat{x}_t) & \text{if } z_t = z_i, \hat{z}_t = z_i \\
\frac{1}{\ell-1} \psi(x_i, \hat{x}_t) & \text{if } z_t = z_i, \hat{z}_t \neq z_i
\end{array} \right.
\]
Therefore,
\[
|\gamma(x_i, z_i, S(i)) - \gamma(x_i, z_i, \hat{S}_t(i))| \leq \frac{2}{\ell - 1}
\]
This completes the proof.

**Lemma 3 (McDiarmid’s Inequality).** Let \( X_1, X_2, \ldots, X_n \) be independent random variables taking values in a set \( \mathbb{X} \). Suppose that \( f : \mathbb{X}^n \to \mathbb{R} \) satisfies
\[
\sup_{x_1, \ldots, x_n, \hat{x}_j \in \mathbb{X}} |f(x_1, \ldots, x_n) - f(x_1, \ldots, \hat{x}_j, \ldots, x_n)| \leq c_j
\]
for constants $c_j, 1 \leq j \leq n$. Then for every $\epsilon > 0$,
\[
\Pr[f(X_1, \ldots, X_n) - Ef \geq \epsilon] \leq \exp \left( \frac{-2\epsilon^2}{\sum_{j=1}^n c_j^2} \right).
\]

**Proof of Theorem 4:** Consider the loss function
\[
g(x, z, S) = \begin{cases} 
1, & \text{if } \gamma(x, z, S) \leq 0, \\
\frac{\alpha - \gamma(x, z, S)}{\alpha}, & \text{if } 0 < \gamma(x, z, S) \leq \alpha, \\
0, & \text{otherwise}.
\end{cases}
\]

It is not difficult to show that
\[
\Pr_{f}[z \neq f_S(x)|S] \leq \mathbb{E}_{F|S}[g(x, z, S)],
\]
where the equality holds when $\alpha = 0$. Hence it suffices to show that $\mathbb{E}_{F|S}[g(x, z, S)]$ is bounded by the right side of (16).

We break $\mathbb{E}_{F|S}[g(x, z, S)] - \frac{1}{\ell} \sum_{i=1}^\ell \xi_i = \mathbb{E}_{F|S}[g(x, z, S)] - \frac{1}{\ell} \sum_{i=1}^\ell g(x_i, z_i, S(i))$ into $A + B + C$:
\[
A = \mathbb{E}_{F|S}[g(x, z, S)] - \mathbb{E}_{F|S} \left[ \frac{1}{\ell} \sum_{i=1}^\ell g(x, z, S(i)) \right],
\]
\[
B = \mathbb{E}_{F|S} \left[ \frac{1}{\ell} \sum_{i=1}^\ell g(x, z, S(i)) \right] - \mathbb{E}_{F}[g(x_j, z_j, S(j))],
\]
\[
C = \mathbb{E}_{F}[g(x_j, z_j, S(j))] - \frac{1}{\ell} \sum_{i=1}^\ell g(x_i, z_i, S(i)),
\]
where $(x_j, z_j)$ is any fixed sample in $S$.

We first look at $A$. It is straightforward to show that
\[
|g(x, z, S) - g(x, z, S(i))| \leq \frac{1}{\alpha} |\gamma(x, z, S) - \gamma(x, z, S(i))| \leq \frac{2}{\ell \alpha},
\]
where the last inequality is based on (A.3). Therefore
\[
A = \mathbb{E}_{F|S} \left\{ \frac{1}{\ell} \sum_{i=1}^\ell [g(x, z, S) - g(x, z, S(i))] \right\} 
\leq \mathbb{E}_{F|S} \left\{ \frac{1}{\ell} \sum_{i=1}^\ell |g(x, z, S) - g(x, z, S(i))| \right\} \leq \frac{2}{\ell \alpha}. \quad (A.6)
\]

Next, we look at $B$. It is not difficult to verify that
\[
\mathbb{E}_{F} \left\{ \mathbb{E}_{F|S} \left[ \frac{1}{\ell} \sum_{i=1}^\ell g(x, z, S(i)) \right] \right\} = \mathbb{E}_{F}[g(x_j, z_j, S(j))].
\]
For a change of one \((x_t, z_t)\) to \((\bar{x}_t, \bar{z}_t)\), we denote
\[
\hat{S}_t = \{(x_1, z_1), \ldots, (x_{t-1}, z_{t-1}), (x_t, \bar{z}_t), (x_{t+1}, z_{t+1}), \ldots, (x_{\ell}, z_{\ell})\}.
\]
From (A.4) we have for any \(z \in K\)
\[
|g(x, z, S(i)) - g(x, z, \hat{S}_t(i))| \leq \frac{1}{\alpha} |\gamma(x, z, S(i)) - \gamma(x, z, \hat{S}_t(i))| \leq \frac{2}{\alpha(\ell - 1)}.
\]
Therefore,
\[
\sup_{(x_1, z_1), \ldots, (x_{\ell}, z_{\ell}), (\bar{x}_t, \bar{z}_t)} \left| \mathbb{E}_F[g(x, z, S(i))] - \mathbb{E}_F[g(x, z, \hat{S}_t(i))] \right| = \sup_{(x_1, z_1), \ldots, (x_{\ell}, z_{\ell}), (\bar{x}_t, \bar{z}_t)} \left| \frac{1}{\ell} \sum_{i=1}^{\ell} g(x, z, S(i)) - \frac{1}{\ell} \sum_{i=1}^{\ell} g(x, z, \hat{S}_t(i)) \right| \leq \frac{2}{\alpha(\ell - 1)}. \tag{A.7}
\]
By (A.7), we apply the McDiarmid’s inequality to get
\[
\Pr(B > \epsilon_1) \leq \exp \left( -\frac{\alpha^2 \epsilon_1^2}{2} \right). \tag{A.8}
\]
Next, we look at \(C\). It is clear that
\[
\mathbb{E}_F \left[ \frac{1}{\ell} \sum_{i=1}^{\ell} g(x_i, z_i, S(i)) \right] = \mathbb{E}_F[g(x_j, z_j, S(j))].
\]
Let \(\bar{g}(S) = \frac{1}{\ell} \sum_{i=1}^{\ell} g(x_i, z_i, S(i))\). For a change of one \((x_t, z_t)\) to \((\bar{x}_t, \bar{z}_t)\), denote
\[
\check{S}_t = \{(x_1, z_1), \ldots, (x_{t-1}, z_{t-1}), (\bar{x}_t, \bar{z}_t), (x_{t+1}, z_{t+1}), \ldots, (x_{\ell}, z_{\ell})\}.
\]
For any \(i \neq t\), it follows from (A.5) that for any \(z_i \in K\)
\[
|g(x_i, z_i, S(i)) - g(x_i, z_i, \check{S}_t(i))| \leq \frac{1}{\alpha} |\gamma(x_i, z_i, S(i)) - \gamma(x_i, z_i, \check{S}_t(i))| \leq \frac{2}{\alpha(\ell - 1)}.
\]
Therefore,
\[
\sup_{(x_1, z_1), \ldots, (x_{\ell}, z_{\ell}), (\bar{x}_t, \bar{z}_t)} \left| \bar{g}(S) - \bar{g}(\check{S}_t) \right| \leq \frac{1}{\ell} + \frac{2}{\alpha(\ell - 1)}. \tag{A.9}
\]
27
By (A.9), we apply the McDiarmid’s inequality to get

$$\Pr(C > \epsilon_2) \leq \exp \left( \frac{-2\epsilon_2^2}{(1 + \frac{2}{\alpha})^2} \right).$$  \tag{A.10}$$

Finally, setting

$$\exp \left( \frac{-\gamma^2 \ell \epsilon_1^2}{2} \right) = \exp \left( \frac{-2\epsilon_2^2}{(1 + \frac{2}{\alpha})^2} \right) = \delta$$

and solving for $\epsilon_1$ and $\epsilon_2$, we obtain

$$\epsilon_1 = \frac{1}{\alpha} \sqrt{\frac{2 \ln(2/\delta)}{\ell}}, \quad \epsilon_2 = \left( \frac{1}{2} + \frac{1}{\alpha} \right) \sqrt{\frac{2 \ln(2/\delta)}{\ell}}.$$

Because $B + C > \epsilon_1 + \epsilon_2$ implies $B > \epsilon_1$ or $C > \epsilon_2$,

$$\Pr(B + C > \epsilon_1 + \epsilon_2) \leq \Pr(B > \epsilon_1 \text{ or } C > \epsilon_2) \leq \Pr(B > \epsilon_1) + \Pr(C > \epsilon_2) \leq \delta.$$

So, with probability at least $1 - \delta$, $B + C \leq \epsilon_1 + \epsilon_2$. Because $A \leq \frac{2}{\ell^2}$, $B + C \leq \epsilon_1 + \epsilon_2$ implies that $A + B + C \leq \epsilon_1 + \epsilon_2 + \frac{2}{\ell^2}$. Therefore, with probability at least $1 - \delta$, $A + B + C \leq \epsilon_1 + \epsilon_2 + \frac{2}{\ell^2}$, i.e.

$$\mathbb{E}_{F|S}[g(x, z, S)] \leq \frac{1}{\ell} \sum_{i=1}^{\ell} g(x_i, z_i, S(i)) + \frac{2}{\ell^2} + \left( 1 + \frac{4}{\alpha} \right) \sqrt{\frac{\ln(2/\delta)}{2\ell}}.$$

It is easy to verify that $\frac{1}{\ell} \sum_{i=1}^{\ell} g(x_i, z_i, S(i)) = \frac{1}{\ell} \sum_{i=1}^{\ell} \frac{\xi_i}{\alpha}$. Therefore, with probability at least $1 - \delta$,

$$\mathbb{E}_{F|S}[g(x, z, S)] \leq \frac{1}{\ell} \sum_{i=1}^{\ell} \frac{\xi_i}{\alpha} + \frac{2}{\ell^2} + \left( 1 + \frac{4}{\alpha} \right) \sqrt{\frac{\ln(2/\delta)}{2\ell}}.$$

This completes the proof. \qed

References


