Transductive Bounds for the Multi-class Majority Vote Classifier
Vasilii Feofanov, Emilie Devijver, Massih-Reza Amini

To cite this version:

Vasilii Feofanov, Emilie Devijver, Massih-Reza Amini. Transductive Bounds for the Multi-class Majority Vote Classifier. 2019. hal-01980449
Transductive Bounds for the Multi-class Majority Vote Classifier

Vasilii Feofanov  Emilie Devijver
Massih-Reza Amini
University Grenoble Alpes, Grenoble INP
LIG, CNRS, Grenoble 38000, France
firstname.lastname@univ-grenoble-alpes.fr

Abstract

In this paper, we propose a transductive bound over the risk of the majority vote classifier learned with partially labeled data for the multi-class classification. The bound is obtained by considering the class confusion matrix as an error indicator and it involves the margin distribution of the classifier over each class and a bound over the risk of the associated Gibbs classifier. When this latter bound is tight and, the errors of the majority vote classifier per class are concentrated on a low margin zone; we prove that the bound over the Bayes classifier’ risk is tight. As an application, we extend the self-learning algorithm to the multi-class case. The algorithm iteratively assigns pseudo-labels to a subset of unlabeled training examples that have their associated class margin above a threshold obtained from the proposed transductive bound. Empirical results on different data sets show the effectiveness of our approach compared to the same algorithm where the threshold is fixed manually, to the extension of TSVM to multi-class classification and to a graph-based semi-supervised algorithm.

1 Introduction

In many real-life applications, the labeling of training examples for learning is costly and sometimes even not realistic. For example, in medical diagnosis or biological data analysis, labeling data may require very expensive tests so that only small labeled data sets are generally available. In many other cases, like web oriented applications, huge amount of observations arrive sequentially and there is not enough time to label data for different information needs; while unlabeled data are abundant.

Learning with labeled and unlabeled data, or semi-supervised learning, has been a subject of growing interest in the machine learning community over the last twenty years [Chapelle et al., 2010]. In this case, labeled training examples are generally assumed to be very few, leading to an inefficient supervised model, while unlabeled training examples
contain valuable information about the prediction problem and it is generally expected that their exploitation leads to an increase of prediction performance.

Considering an input space $\mathcal{X} \subset \mathbb{R}^d$ and a discrete output space $\mathcal{Y}$, we assume available a set of labeled training examples $Z_L = \{(x_i, y_i)\}_{i=1}^l \in (\mathcal{X} \times \mathcal{Y})^l$, identically and independently distributed (i.i.d.) with respect to a fixed yet unknown probability distribution $\mathcal{D}$ over $\mathcal{X} \times \mathcal{Y}$, and a set of unlabeled training examples $X_U = \{x_i\}_{i=l+1}^{l+u} \in \mathcal{X}^u$ supposed to be drawn i.i.d. from the marginal distribution $P_X(x)$, over the domain $\mathcal{X}$. If $X_U$ is empty, then the problem reduces to supervised learning. The other extreme case is the situation where $Z_L$ is empty and which corresponds to unsupervised learning.

Most studies in semi-supervised learning have focused on the binary classification problem, whereas just few ones are devoted to the multi-class framework, i.e. $|\mathcal{Y}| > 2$ with some recent studies considering the learnability of multi-class semi-supervised learning algorithms under some specific assumptions. For example, Maximov et al. [2018] proved the consistency of the Empirical Risk Minimization principle in some cases by bounding the true risk of the trained classifier. However such bounds are not usable in practice as they are generally too loose.

In this paper, we propose a transductive bound for the multi-class majority vote classifier, which to the best of our knowledge, is a first attempt in this direction. The bound is based on the risk of the associated Gibbs classifier and by considering the class confusion matrix as an error indicator as proposed in Morvant et al. [2012]. This bound is obtained by analytically solving a linear program and it comes out that in the case where the bound over the risk of the Gibbs classifier is tight and when the Bayes classifier makes most of its errors on low margin examples, the obtained bound is tight. From this result, we then propose to automatically find a threshold for which the risk of the majority vote classifier is the lowest. This finding allows to consider the output of the Bayes classifier, or its margin, as an indicator of confidence and to extend self-learning algorithms to the multi-class case. The proposed strategy iteratively learns a Bayes classifier by assigning at each iteration pseudo-labels to unlabeled examples having their margin above a certain threshold obtained from the proposed transductive bound.

The paper is organized as follows. In Section 2, we introduce the problem statement and the proposed framework. In Section 3, we present a bound over the transductive risk of the multi-class majority vote classifier. In Section 4, we present empirical evidence showing that the extended self-learning algorithm learned using the proposed bound is effective compared to the same algorithm where the threshold is fixed manually, to the extension of TSVM to multi-class classification and to a graph-based semi-supervised algorithm on difference data sets. Finally, in Section 5, we discuss the outcomes of this study and give some pointers to further research.

2 Framework and Definitions

In this study, we consider learning algorithms that work in a fixed hypothesis space $\mathcal{H} = \{h : \mathcal{X} \to \mathcal{Y}\}$ of multi-class classifiers (defined without reference to the training data). After observing the training set $S = Z_L \cup X_U$, the task of the learner is then to
choose a posterior distribution $Q$ over $H$ such that the $Q$-weighted majority vote classifier (also called Bayes classifier)

$$B_Q(x) := \arg\max_{c \in \mathcal{Y}} \left[ \mathbb{E}_{h \sim Q} \mathbb{1}_{h(x) = c} \right], \quad \forall x \in \mathcal{X},$$

(1)

will have the smallest possible risk on examples of $X_U$. Together with that, we consider the associated Gibbs classifier $G_Q$ that for any $x \in \mathcal{X}$ chooses randomly a classifier $h \in H$ according to $Q$. We accordingly define the transductive error rate of $B_Q$ and $G_Q$ over an unlabeled set by:

$$E_U(B_Q) := \frac{1}{u} \sum_{x' \in X_U} \mathbb{1}_{B_Q(x') \neq y'},$$

(2)

$$E_U(G_Q) := \frac{1}{u} \sum_{x' \in X_U} \mathbb{E}_{h \sim Q} \mathbb{1}_{h(x') \neq y'}.$$  

(3)

For an observation $x$, we further define its unsigned margin $m_x = (m_Q(x, c))_{c=1}^K$ which measures the confidence in each class of the classifier as

$$m_Q(x, y) := \mathbb{E}_{h \sim Q} \mathbb{1}_{h(x) = y}.$$  

(4)

The proposed bound follows a bound on the joint Bayes error rate which given a vector $\theta = (\theta_n)_{n=1}^K \in [0, 1]^K$, is defined as,

$$E_{U, \theta}(B_Q) := \frac{1}{u} \sum_{x' \in X_U} \mathbb{1}_{B_Q(x') \neq y'} \mathbb{1}_{m_Q(x', B_Q(x')) \geq \theta_k},$$

where $y'$ is the true unknown class label of $x'$. One of the practical issues that arises from this result is the possibility to define a set of thresholds $\theta$ for which the bound is optimal and that we use in a self-learning algorithm by iteratively assigning pseudo-labels to unlabeled examples having the highest class margin above the corresponding threshold.

However, as we work with multi-class data, the error rate does not describe the dispersion of errors regarding each class over all the others. We rather use the confusion matrix, which provides a richer information. For a classifier $h$, the transductive confusion matrix $C^U_h = (c_{ij})_{i,j=1,...,K}$ is defined as follows:

$$c_{ij} := \begin{cases} 0 & i = j \\ R_U(h, i, j) & i \neq j \end{cases},$$

where for a classifier $h$, for each class pair $(i, j) \in \{1, \ldots, K\}^2$ s.t. $i \neq j$, the transductive conditional risk $R_U$ is defined by:

$$R_U(h, i, j) := \frac{1}{u_i} \sum_{x' \in X_U} \mathbb{1}_{h(x') = j} \mathbb{1}_{y' = i},$$

with $u_i = \sum_{x' \in X_U} \mathbb{1}_{y' = i}$ is the size of class $i \in \mathcal{Y}$. 

3
Similarly, the transductive conditional Gibbs risk is defined as

$$R(G_Q, i, j) := E_{h \sim Q} R(h, i, j).$$

The transductive joint Bayes confusion matrix $C_{BQ}^{\theta, Q} = (c_{ij})_{i,j=(1, \ldots, K)^2}$ given a vector $\theta = (\theta_n)_{n=1}^K$, $\theta \in [0, 1]^K$ is defined as:

$$c_{ij} :=
\begin{cases}
0 & i = j, \\
R_{\theta, BQ}(i, j) & i \neq j,
\end{cases}$$

where the transductive joint Bayes conditional risk $R_{\theta, BQ}(i, j)$ for the class pair $(i, j) \in \{1, \ldots, K\}^2$ s.t. $i \neq j$, is defined as follows:

$$R_{\theta, BQ}(i, j) := \frac{1}{u_i} \sum_{x' \in X_i} \mathbb{I}_{BQ(x') = j} \mathbb{I}_{y' = i} \mathbb{I}_{m_Q(x', j) \geq \theta_j}.$$

Thus, the transductive joint Bayes conditional risk counts an example as wrongly classified, if its true label is $i$ and the majority vote classifier predicts the class $j$ with the margin $m_Q(x', j) \geq \theta_j$. Generally, the majority vote classifier is supposed to make errors by predicting the label $j$ mostly on examples with a low value of $m_Q(x', j)$. Then, if $\theta_j$ is high enough, the joint conditional risk computes the probability to make a mistake on high margin "confident" observations.

To work with matrices, we use the spectral norm, defined by, for a matrix $A$ of size $n \times m$:

$$\|A\|_2 := \sup_{x \in \mathbb{R}^m} \|Ax\|_2 = \sup_{x \in \mathbb{R}^m} \frac{\|Ax\|_2}{\|x\|_2}.$$  

It corresponds to the matrix’s largest singular value.

We conclude this section by the following proposition, which links the error rate to the confusion matrix.

**Proposition 1.** Let $B_Q$ be the Bayes classifier. Given a vector $\theta \in [0, 1]^K$, for $p := \{u_i/u\}_{i=1}^K$, we have:

$$\mathbb{E}_{\theta, BQ} = \left( C_{BQ}^{\theta, Q} \right)^\top p_1.$$

### 3 Transductive Bounds on the risk of the Multi-class Majority Vote Classifier

In this section we propose a transductive bound for the majority vote classifier in multi-class setting. The bound is based on the margin distribution as well as a bound of the transductive conditional Gibbs risk, which we suppose given. First, we give a theorem that provides a bound for the transductive joint Bayes conditional risk, which leads to a bound for the transductive conditional risk of the majority vote classifier. Then, a corollary is derived, proposing upper bounds for the Bayes confusion matrix and the Bayes error rate. Finally, we propose a setting under which the bound on the conditional risk of the Bayes classifier becomes tight.
Main Result

**Theorem 1.** Let $B_Q$ be the $Q$-weighted majority vote classifier. Suppose an upper bound of the transductive conditional Gibbs risk $R_u(G_Q, i, j)$ that holds with probability $1 - \delta$ is given. Then for any $Q$ and $\forall \delta \in (0, 1], \forall \theta \in [0, 1]^K$, $\forall (i, j) \in \mathcal{Y}^2$, with probability at least $1 - \delta$ we have:

$$R_u(B_Q, i, j) \leq \inf_{\gamma \in [0, 1]} \left\{ I_{i,j}^{(\leq \gamma)}(0, \gamma) + \frac{1}{\gamma} \left[ (K_{i,j}^\delta - M_{i,j}^\gamma(\gamma)) \right]_+ \right\}, \quad (5)$$

$$R_{u,\theta}(B_Q, i, j) \leq \inf_{\gamma \in [\theta, 1]} \left\{ I_{i,j}^{(\leq \gamma)}(\theta, \gamma) + \frac{1}{\gamma} \left[ (K_{i,j}^\delta - M_{i,j}^\gamma(\gamma)) + M_{i,j}^\gamma(\theta) \right]_+ \right\}, \quad (6)$$

where

$$K_{i,j}^\delta = R_u(G_Q, i, j) - \varepsilon_{i,j},$$

$$\varepsilon_{i,j} = \frac{1}{u_i} \sum_{x' \in X_{iQ}} \mathbb{1}_{B_Q(x') \neq j} \mathbb{1}_{y' = i} m_Q(x', j),$$

$$I_{i,j}^{(\leq \gamma)}(0, \gamma) = \frac{1}{u_i} \sum_{x' \in X_{iQ}} \mathbb{1}_{y' = i} \mathbb{1}_{t \leq m_Q(x', j) < 2 \gamma},$$

$$I_{i,j}^{(\leq \gamma)}(\theta, \gamma) = \frac{1}{u_i} \sum_{x' \in X_{iQ}} \mathbb{1}_{y' = i} \mathbb{1}_{t \leq m_Q(x', j) < 2 \gamma} \theta,$$

$$M_{i,j}^\gamma(t) = \frac{1}{u_i} \sum_{x' \in X_{iQ}} \mathbb{1}_{y' = i} \mathbb{1}_{m_Q(x', j) < t} m_Q(x', j),$$

$$\left[ x \right]_+ = x \cdot 1_{x > 0},$$

From spectral norm properties, the following corollary is easily deduced:

**Corollary 1.** Let $U_{ij}^\delta(\theta)$ be the upper bound for the transductive joint Bayes conditional risk from **Theorem 1** that holds $\forall (i, j) \in \mathcal{Y}^2, \forall \delta \in (0, 1], \forall \theta \in [0, 1]^K$, with probability at least $1 - \delta$:

$$U_{ij}^\delta(\theta) := \inf_{\gamma \in [\theta, 1]} \left\{ I_{i,j}^{(\leq \gamma)}(\theta, \gamma) + \frac{1}{\gamma} \left[ (K_{i,j}^\delta - M_{i,j}^\gamma(\gamma)) + M_{i,j}^\gamma(\theta) \right]_+ \right\}. \quad (7)$$

Introduce the confusion matrix $U_{ij}^\delta$ which $(i, j)$-entry is 0, if $i = j$, and $U_{ij}^\delta(\theta)$ otherwise. We consider the spectral norm. Then, we have:

$$\| C_{ij}^{\theta} \| \leq \| U_{ij}^\delta \| \quad \text{and} \quad \| C_{ij}^{\theta} \| \leq \| U_{ij}^\delta \|,$$

where $0_K$ is the $K$-size vector of zeros.

Moreover, we have:

$$E_{u,\theta}(B_Q) \leq \| (U_{ij}^\delta) \|_1 \quad \text{and} \quad E_{u}(B_Q) \leq \| (U_{ij}^\delta) \|_1,$$

where $p = \{u_i/u\}_{i=1}^K$. 

5
In the following proposition, we assume that the classifier makes most of its error on unlabeled examples with low margin. Then, considering that the margin is an indicator of confidence, the bound becomes tight.

**Proposition 2.** For all $\mathbf{x}' \in \mathbf{X_U}$ there exists $C \in [0, 1]$ such that for all $(i, j) \in \mathcal{Y}^2$, for all $\gamma > 0$:

$$\frac{1}{u_i} \sum_{\mathbf{x}' \in \mathbf{X_U}} \mathbb{1}_{B_{Q}(\mathbf{x}') = j} \mathbb{1}_{y' = i} \mathbb{1}_{m_Q(\mathbf{x}', j) = \gamma} \neq 0 \Rightarrow \frac{1}{u_i} \sum_{\mathbf{x}' \in \mathbf{X_U}} \mathbb{1}_{B_{Q}(\mathbf{x}') = j} \mathbb{1}_{y' = i} \mathbb{1}_{m_Q(\mathbf{x}', j) < \gamma} \geq C \cdot \frac{1}{u_i} \sum_{\mathbf{x}' \in \mathbf{X_U}} \mathbb{1}_{y' = i} \mathbb{1}_{m_Q(\mathbf{x}', j) < \gamma}.$$  

(8)

Then, with probability at least $1 - \delta$ the following inequality holds:

$$F_{i,j}^\delta - R_{u}(B_{Q}, i, j) \leq \frac{1 - C}{C} R_{u}(B_{Q}, i, j) + \frac{R_{u}^\delta(G_{Q}, i, j) - R_{u}(G_{Q}, i, j)}{\gamma^*},$$

(9)

where

- $\gamma^* := \gamma^{(p)}$, where $p := \sup \left\{ w \in \{1, \ldots, N_j\} | b_{i,j}^{(w)} \neq 0 \right\}$.
- $F_{i,j}^\delta := \inf_{\gamma \in [0, 1]} \left\{ I_{i,j}^{(\leq)}(0, \gamma) + \frac{1}{\gamma} \left[ (K_{i,j}^\delta - M_{i,j}^\leq(\gamma)) \right]_+ \right\}$.

In the next section, proofs are provided.

**Proofs**

**Proof of Theorem:** This proof relies on two lemmas. The first one connects the conditional Gibbs risk and the conditional joint Bayes risk. The second one provides an analytic solution of a linear program.

**Lemma 1.** Let $\Gamma_c := \{ \gamma_c | \exists \mathbf{x}' \in \mathbf{X_U} : \gamma_c = m_Q(\mathbf{x}', c) \}$, where $c \in \mathcal{Y}$, and $N_c := |\Gamma_c|$. Let enumerate its elements such that they form an ascending order:

$$\gamma_c^{(1)} \leq \gamma_c^{(2)} \leq \cdots \leq \gamma_c^{(N_c)}.$$

Denote $b_{i,j}^{(n)} := \frac{1}{u_i} \sum_{\mathbf{x}' \in \mathbf{X_U}} \mathbb{1}_{B_{Q}(\mathbf{x}') = j} \mathbb{1}_{y' = i} \mathbb{1}_{m_Q(\mathbf{x}', j) = \gamma_c^{(n)}}$. Then, $\forall (i, j) \in \mathcal{Y}^2$:

$$R_{u}(G_{Q}, i, j) = \sum_{n=1}^{N_j} b_{i,j}^{(n)} \gamma_c^{(n)} + \varepsilon_{i,j},$$

(10)

$$R_{u\cap\theta}(B_{Q}, i, j) = \sum_{n=k+1}^{N_j} b_{i,j}^{(n)},$$

(11)

where
• \( \varepsilon_{i,j} = \frac{1}{u_i} \sum_{x' \in X_u} \mathbb{1}_{B_Q(x') \neq j} \mathbb{1}_{y' = i} m_Q(x', j) \)

• \( k = \begin{cases} 0 & \text{if } \{n|\gamma_{j}^{(n)} < \theta_j\} = \emptyset \\ \max\{n|\gamma_{j}^{(n)} < \theta_j\} & \text{otherwise.} \end{cases} \)

Proof. Formula (10) is derived through conditioning by the value of the majority vote classifier.

Formula (11) is get by considering \( k \), the index of the smallest \( \gamma \) larger than the threshold \( \theta \):

\[
R_{U \cup \theta}(B_Q, i, j) = \frac{1}{u_i} \sum_{n=k+1}^{N_j} \sum_{x' \in X_u} \mathbb{1}_{B_Q(x') = j} \mathbb{1}_{y' = i} m_Q(x', j)_{\gamma_{j}^{(n)}}.
\]

We conclude by definition of \( b_{i,j}^{(n)} \).

Lemma 2 (Lemma 4 in Amini et al. [2008]). Let \( (g_i)_{i \in \{1, \ldots, N\}} \) be such that \( 0 < g_1 < g_2 < \cdots < g_{N-1} < g_N \leq 1 \). Consider also \( p_i \geq 0, i = 1, \ldots, N, B \geq 0, k \in \{1, \ldots, N\} \). Then, the optimal solution of the linear program:

\[
\begin{align*}
\max_{q_i = (q_1, \ldots, q_N)} & F(q) := \max_{q_1, \ldots, q_N} \sum_{i=k+1}^{N} q_i \\
0 & \leq q_i \leq p_i \quad \forall i \in \{1, \ldots, N\} \\
\sum_{i=1}^{N} q_i g_i & \leq B
\end{align*}
\]

will be \( q^* \) defined as \( \forall i \leq k : q_i^* = 0, \forall i > k : q_i^* = \min \left( p_i, \left[ \frac{B - \sum_{j<i} q_j g_j}{g_i} \right]_+ \right) \).

Now we combine those two lemmas to prove Theorem 1.

First, notice that Eq. (5) is easily derived from Eq. (6) using that \( M_{i,j}^{<}(0) = 0 \).

To prove Eq. (6), we consider two cases.

First, \( \forall (i,j), \forall \theta \in [0,1]^K \), when the mistake is maximized, using Lemma 2, we get:

\[
R_{U \cup \theta}(B_Q, i, j) = \sum_{n=k}^{N_j} b_{i,j}^{(n)} \leq \max_{b_{i,j}^{(1)}, \ldots, b_{i,j}^{(N_j)}} \sum_{n=k}^{N_j} b_{i,j}^{(n)},
\]

with \( k \) is equal to 0 when \( \{n|\gamma_{j}^{(n)} < \theta_j\} = \emptyset \), and \( \max\{n|\gamma_{j}^{(n)} < \theta_j\} \) otherwise.

Consider the upper bound \( R^u_{i,j}(G_Q, i, j) \) of the Gibbs conditional risk \( R_{U}(G_Q, i, j) \) that holds with probability \( 1 - \delta \). Denote \( K_{i,j}^{\delta} = R^u_{i,j}(G_Q, i, j) - \varepsilon_{i,j} \) and \( B_{i,j}^{(n)} = \frac{1}{u_i} \sum_{x' \in X_u} \mathbb{1}_{y' = i} m_Q(x', j)_{\gamma_{j}^{(n)}} \). We are interested in the following linear program task:

\[
\begin{align*}
\max & \sum_{n=k}^{N_j} b_{i,j}^{(n)} \\
\text{s.t.} & \forall n, 0 \leq b_{i,j}^{(n)} \leq B_{i,j}^{(n)} \text{ and } \sum_{n=1}^{N_j} b_{i,j}^{(n)} \gamma_{j}^{(n)} \leq K_{i,j}^{\delta},
\end{align*}
\]

7
As $\sum_{k<w<n} \gamma_{j}^{(w)} B_{i,j}^{(w)} = M_{i,j}^\leq (\gamma_{j}^{(n)}) - M_{i,j}^\leq (\theta_{j})$ with $k = \max\{w\gamma_{j}^{(w)} < t\}$, we get the following solution of the linear program [13] by using Lemma [2] with $p = \max\{n|K_{i,j}^\delta - M_{i,j}^\leq (\gamma_{j}^{(n)}) + M_{i,j}^\leq (\theta_{j}) > 0\}$, 

$$
\begin{cases}
0 & n \leq k, \\
\frac{1}{\gamma_{j}^{(p)}} (K_{i,j}^\delta - M_{i,j}^\leq (\gamma_{j}^{(p)}) + M_{i,j}^\leq (\theta_{j})) & n = p, \\
0 & n > p.
\end{cases}
$$

This formulae is used to rewrite Eq. [12], as $\sum_{n=k+1}^{p-1} B_{i,j}^{(n)} = I_{i,j}^{(\leq,<)} (\theta_{j}, \gamma_{j})$:

$$
R_{U\cap \theta}(B_{Q}, i, j) \leq I_{i,j}^{(\leq,<)} (\theta_{j}, \gamma_{j}) + \frac{1}{\gamma_{j}^{(p)}} (K_{i,j}^\delta - M_{i,j}^\leq (\gamma_{j}^{(p)}) + M_{i,j}^\leq (\theta_{j})).
$$

Consider the function: $\gamma \mapsto T_{i,j}(\gamma) := I_{i,j}^{(\leq,<)} (\theta_{j}, \gamma) + \frac{1}{\gamma_{j}^{(p)}} (K_{i,j}^\delta - M_{i,j}^\leq (\gamma_{j}^{(p)}) + M_{i,j}^\leq (\theta_{j}))$. To prove the theorem, it remains to check that $\forall \gamma \in [\theta_{j}, 1]$, $T_{i,j}(\gamma_{j}^{(p)}) \leq T_{i,j}(\gamma_{j})$. For this, let’s consider $\gamma_{j}^{(w)}$, $w \in \{1, \ldots, N_{j}\}$.

If $w > p$, then

$$
T_{i,j}(\gamma_{j}^{(p)}) \leq I_{i,j}^{(\leq,<)} (\theta_{j}, \gamma_{j}^{(p)}) \leq T_{i,j}(\gamma_{j}^{(w)}).
$$

If $w < p$, then

$$
T(\gamma_{j}^{(p)}) - T(\gamma_{j}^{(w)}) = \sum_{n=w}^{p} b_{i,j}^{(n)} - \frac{1}{\gamma_{j}^{(w)}} (K_{i,j}^\delta - M_{i,j}^\leq (\gamma_{j}^{(w)}) + M_{i,j}^\leq (\theta_{j}))
\begin{aligned}
= & \sum_{n=w}^{p} b_{i,j}^{(n)} - \frac{1}{\gamma_{j}^{(w)}} \left( \sum_{n=k+1}^{p} b_{i,j}^{(n)} \gamma_{j}^{(n)} - \sum_{n=k+1}^{w-1} \gamma_{j}^{(n)} b_{i,j}^{(n)} \right) \\
= & \frac{1}{\gamma_{j}^{(w)}} \left( \sum_{n=w}^{p} b_{i,j}^{(n)} \gamma_{j}^{(w)} - \sum_{n=w}^{p} b_{i,j}^{(n)} \gamma_{j}^{(n)} \right) \leq 0.
\end{aligned}
$$

Summing up, we derive for $R_{U\cap \theta}(B_{Q}, i, j)$ the upper bound $T_{i,j}(\gamma_{j}^{(p)})$, which, in addition, is the infimum of $T_{i,j}$ on $\gamma \in [\theta_{j}, 1]$. 

\[ \square \]

**Proof of Proposition \[3\]** First, let’s show that, $\forall (i, j) \in \mathcal{Y}$,

$$
R_{U}(B_{Q}, i, j) \geq \frac{1}{u_{i}} \sum_{x' \in X_{i}} I_{B_{Q}(x')} = 1_{y' = 1_{m_{Q}(x')} < \gamma^{*}} + \frac{1}{\gamma^{*}} [K_{i,j} - M_{i,j}^\leq (\gamma^{*})]_{+}, \quad (14)
$$

where $K_{i,j} = R_{U}(G_{Q}, i, j) - \varepsilon_{i,j}$ and $\varepsilon_{i,j} = \frac{1}{u_{i}} \sum_{x' \in X_{i}} I_{B_{Q}(x') \neq j} 1_{y' = 1_{m_{Q}(x', j)}}$.

Denote $\gamma^{*} = \gamma_{j}^{(p)}$. We apply Lemma \[1\] and get that $R_{U}(G_{Q}, i, j) = \sum_{n=1}^{p} b_{i,j}^{(n)} \gamma_{j}^{(n)} + \varepsilon_{i,j}$, where $b_{i,j}^{(n)} := \frac{1}{u_{i}} \sum_{x' \in X_{i}} I_{B_{Q}(x') = j} 1_{y' = i} 1_{m_{Q}(x', j) = \gamma_{j}^{(n)}}$. Then, we can write $b_{i,j}^{(p)} = \ldots.
In addition, since for any non-negative real numbers $a, b, m$ from Eq. (14):

\[ b_{i,j}^p \geq \frac{1}{\gamma_j} [K_{i,j} - M_{i,j}^\leq (\gamma_j^*)]_+. \]

Also, taking into account Lemma 1, one can notice that $R_d(B_Q, i, j) = \sum_{n=1}^p b_{i,j}^{(n)} = b_{i,j}^p + \frac{1}{\gamma_j} \sum_{x' \in X_d} 1_{B_Q(x')=j} 1_{y'=1} 1_{m_Q(x', j) < \gamma^*}$. Combining this fact and Eq. (15) we deduce Eq. (14).

Using the initial assumptions and following the definition of $I_{i,j}^{(q_1, q_2)}(t, s)$ we deduce from Eq. (14):

\[ R_d(B_Q, i, j) \geq C \cdot I_{i,j}^{(\leq \leq <)}(0, \gamma^*) + \frac{1}{\gamma_j} [K_{i,j} - M_{i,j}^\leq (\gamma_j^*)]_+. \]

Notice that $F_{i,j}^\leq \leq I_{i,j}^{(\leq \leq <)}(0, \gamma^*) + \frac{1}{\gamma_j} \left( [K_{i,j}^\leq - M_{i,j}^\leq (\gamma_j^*)]_+ - [K_{i,j} - M_{i,j}^\leq (\gamma^*)]_+ \right)$.

which holds with probability $1 - \delta$.

Then, as by definition $R_{i,j}^G(G_Q) \geq R_d(G_Q)$ holds with probability $1 - \delta$, we obtain:

\[ K_{i,j}^\leq - K_{i,j} = R_{i,j}^G(G_Q, i, j) - R_d(G_Q, i, j) \geq 0. \]

In addition, since for any non-negative real numbers $a, b, m \in \mathbb{R}^+$ with $b \geq a$, it is true that $[b - m]_+ - [a - m]_+ \leq b - a$, we deduce that

\[ \left( [K_{i,j}^\leq - M_{i,j}^\leq (\gamma_j^*)]_+ - [K_{i,j} - M_{i,j}^\leq (\gamma^*)]_+ \right) \leq R_{i,j}^G(G_Q, i, j) - R_d(G_Q, i, j). \]

Finally, from Eq. (16) we derive that $I_{i,j}^{(\leq \leq <)}(0, \gamma^*) \leq \frac{1}{C} R_d(B_Q, i, j)$. Taking into account this fact as well as Eq. (18), we infer Eq. (9).

Proposition 2 states that if Condition (8) holds, the difference between the conditional Bayes risk and its upper bound does not exceed an expression that depends on a constant $C$. If we assume that the Gibbs conditional risk bound is as tight as possible and the majority vote classifier makes most of its mistake for the class $j$ on observations with the low value of $m_Q(x', j)$, we obtain that Condition (8) accepts a high value $C$ (close to 1), and the bound becomes tight. From theoretical point of view it makes sense to assume that the majority vote classifier mistakes mostly on low margin region, since if the class got a relatively high vote from the hypotheses, we expect that it is predicted correctly.
4 Multi-class Self-Learning Algorithm

Algorithm

Pseudo-labelling is considered in this paper to increase the labeled set and improve performances. We introduce the conditional Bayes error rate $E_{U|\theta}(B_Q)$, defined by:

$$E_{U|\theta}(B_Q) := \frac{E_{U\wedge \theta}(B_Q)}{\pi(m_Q(x',k) \geq \theta_k)},$$

where $\pi(m_Q(x',k) \geq \theta_k) := \frac{1}{u} \sum_{x' \in X_d} I_{m_Q(x',k) \geq \theta_k} k := B_Q(x')$, to make a trade-off between the value of the joint Bayes error rate and the number of pseudo-labeled examples. The numerator reflects proportions of mistakes on the unlabeled set when the threshold is equal to $\theta$, whereas the denominator computes the proportions of unlabeled observations with the margin no less than the threshold for the predicted class. One would use the bound get in Theorem 1 but two algorithmic drawbacks of the theorem have to be highlighted. First, the bound depends on the true labels of the observations. Finally, the theorem assumes that a bound for the Gibbs conditional risk is given. To avoid these issues, we take into consideration the non-deterministic case, namely, we suppose the posterior distribution $P_Y(y|x)$ defined over $Y$. Then, we replace the deterministic $I_{y=i}$ value by the corresponding probabilistic $P_Y(i|x)$ one. In practice, $P_Y(y|x)$ is approximated by $m_Q(x,y)$, saying that the confidence get by the margin are used as probabilities. Remark that if the space describes the problem poorly, the majority vote classifier is not able to give good margins, and then the pseudo-labelling approach can not provide a high increase in performance.

Similarly to the self-learning algorithm introduced in Amini et al. [2008], in practice, to find an optimal $\theta^*$ we perform grid search that is the exhaustive search over the grid of values within the interval $(0,1]$. The same algorithm is used for computing the optimal $\gamma^*$ that provides the value of an upper bound for the conditional risk (see Theorem 1). In contrast to the self-learning algorithm, the direct grid search in the multi-class setting is costly ($O(S^K)$, where $S$ is the sampling rate of the grid). As

$$E_{U\wedge \theta}(B_Q) \leq \sum_{j=1}^{K} \frac{E^{(j)}_{U\wedge \theta}(B_Q)}{\pi\{(m_Q(x',j) \geq \theta_j) \wedge (B_Q(x') = j)\}},$$

where $E^{(j)}_{U\wedge \theta}(B_Q) = \sum_{i=1}^{K} \sum_{u} R_{U\wedge \theta}(B_Q,i,j)$, the sum might be minimized term by term, tuning independently each component of $\theta$. This replaces the $K$-dimensional minimization task by $K$ tasks of 1-dimensional minimization. Then, the time complexity of the threshold search is $O(K^2S^2u)$.

The extended strategy denoted by MLSA is described in Algorithm 1. \footnote{The code source of the algorithm can be found at https://github.com/vfeofanov/trans-bounds-maj-vote}
Multi-class self-learning algorithm (MLSA)

**Input:**
- labeled data set $Z_L$
- Unlabeled observations $X_U$

**Initialisation:**
- A set of pseudo-labeled instances, $Z_U \leftarrow \emptyset$
- A classifier $H$ trained on $Z_L$

**repeat**
1. Compute the margin threshold $\theta^*$ that minimizes the conditional Bayes error rate:
   \[
   \theta^* = \arg\min_{\theta \in (0,1]^K} E_{U|\theta}(B_Q).
   \]
2. $S \leftarrow \{(x', y') | x' \in X_U; [m_Q(x', y') \geq \theta_{y'}] \land [y' = \arg\max_{c \in Y} m_Q(x', c)]\}$
3. $Z_U \leftarrow Z_U \cup S$, $X_U \leftarrow X_U \setminus S$
4. Learn a classifier $H$ with the following loss function:
   \[
   \mathcal{L}(H, Z_L, Z_U) = \frac{l + |Z_U|}{l} \mathcal{L}(H, Z_L) + \frac{l + |Z_U|}{|Z_U|} \mathcal{L}(H, Z_U)
   \]

**until** $X_U$ or $S$ are $\emptyset$

**Output:** The final classifier $H$

---

**Table 1:** Characteristics of data sets used in our experiments ordered by the size of the training set ($|S| = |Z_L| + |X_U|$).

| Data set | # of labeled examples, $|Z_L|$ | # of unlabeled examples, $|X_U|$ | Dimension, $d$ | # of classes, $K$ |
|----------|-------------------------------|---------------------------------|----------------|------------------|
| Vowel    | 99                            | 891                             | 10             | 11               |
| DNA      | 31                            | 3155                            | 180            | 3                |
| Pendigits | 109                           | 10883                           | 16             | 10               |
| MNIST    | 175                           | 69825                           | 900            | 10               |
| SensIT   | 49                            | 98479                           | 100            | 3                |

Experimental Results

In our experiments, we considered the Random Forest model with 200 trees and the maximal depth of trees [Breiman, 2001], denoted by $H$ in Algorithm 1, as the majority voted classifier with uniform posterior distribution. In this case, the margin $m_x$ of an observation is evaluated by the mean vector of votes that the trees of the forest give to each class. As the size of the labeled training examples ($|Z_L|$) is small, we did not tune the hyperparameters of the classifier and left them by their default values.

The proposed MSLA algorithm, with margin thresholds estimated by minimizing the conditional Bayes error rate, is compared with

- a supervised Random Forest (RF) trained using only labeled examples. The ap-
approach is obtained at the initialization step of MSLA and once learned it is directly applied to predict the class labels of the whole unlabeled set;

- a scikit-learn implementation of the graph based, label propagation [Pedregosa et al., 2011] approach (denoted by LP);
- the one-versus-all extension of TSVM [Joachims, 1999] denoted by OVA-TSVM. In some cases, the convergence time was too long, we stopped learning the model when the convergence took more than one hour;
- the multi-class extension of the classical self-learning approach (denoted by FSLA) described in Tür et al. [2005] with the margin thresholds fixed to the best threshold (0.7 for all classes) that we found on the unlabeled set, after testing different values manually over a predefined set of thresholds in the set \{0.1, 0.2, \ldots, 0.9\}.

<table>
<thead>
<tr>
<th>Data set</th>
<th>Score</th>
<th>RF</th>
<th>LP</th>
<th>OVA-TSVM</th>
<th>FSLA_{θ=0.7}</th>
<th>MSLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vowel</td>
<td>ACC</td>
<td>.5832 ± .0261</td>
<td>.5768 ± .0268</td>
<td>NA</td>
<td>.5164 ± .0429</td>
<td>.5918 ± .0267</td>
</tr>
<tr>
<td></td>
<td>F1</td>
<td>.5716 ± .0275</td>
<td>.568 ± .0261</td>
<td>NA</td>
<td>.4934 ± .0459</td>
<td>.5804 ± .0298</td>
</tr>
<tr>
<td>DNA</td>
<td>ACC</td>
<td>.6932 ± .0721</td>
<td>.5383 ± .0387</td>
<td>.8125 ± .0386</td>
<td>.5164 ± .0899</td>
<td>.7059 ± .0826</td>
</tr>
<tr>
<td></td>
<td>F1</td>
<td>.654 ± .1086</td>
<td>.5348 ± .0437</td>
<td>.8119 ± .0375</td>
<td>.3724 ± .0959</td>
<td>.6631 ± .1177</td>
</tr>
<tr>
<td>Pendigits</td>
<td>ACC</td>
<td>.8639 ± .022</td>
<td>.7767 ± .0515</td>
<td>.667 ± .0225</td>
<td>.8474 ± .0352</td>
<td>.8866 ± .019</td>
</tr>
<tr>
<td></td>
<td>F1</td>
<td>.8613 ± .0252</td>
<td>.7564 ± .0687</td>
<td>.6562 ± .0213</td>
<td>.8415 ± .0424</td>
<td>.8851 ± .0198</td>
</tr>
<tr>
<td>MNIST</td>
<td>ACC</td>
<td>.8647 ± .0176</td>
<td>NA</td>
<td>NA</td>
<td>.7998 ± .0587</td>
<td>.9085 ± .0182</td>
</tr>
<tr>
<td></td>
<td>F1</td>
<td>.8633 ± .0193</td>
<td>NA</td>
<td>NA</td>
<td>.7743 ± .077</td>
<td>.9086 ± .0182</td>
</tr>
<tr>
<td>SensIT</td>
<td>ACC</td>
<td>.67 ± .0291</td>
<td>NA</td>
<td>NA</td>
<td>.6192 ± .0366</td>
<td>.6745 ± .0288</td>
</tr>
<tr>
<td></td>
<td>F1</td>
<td>.654 ± .0448</td>
<td>NA</td>
<td>NA</td>
<td>.5784 ± .0638</td>
<td>.6599 ± .0421</td>
</tr>
</tbody>
</table>

Table 2: The result table of the classification performance on different data sets described in Table 1. The performance is computed using two score functions: accuracy and F1. The sign ↓ shows if the performance is statistically worse than the best result on the level 0.01 of significance. NA indicates the case when the algorithm does not converge.

Experiments are conducted on 5 publicly available data sets [Dheeru and Karra Taniskidou, 2017, Chang and Lin, 2011]. The associated applications are image classification, with the MNIST and the Pendigits databases of handwritten digits; a signal processing kind of application with the Vowel data set for vehicle type classification, speech recognition using the Vowel database and finally DNA prediction using the DNA data set. We use available preprocessed versions [Chang and Lin, 2011] of all data sets, except MNIST, for which we extracted HOG-features [Dalal and Triggs, 2005] with the following parameters: cells of size (4, 4), blocks of size (5, 5) and the number of orientations was fixed to 4. The main characteristics of these data sets are summarized in Table 1.

Each experiment is conducted 20 times, by randomly splitting the labeled and the unlabeled training sets from the original data sets by keeping fixed their respective size \(l\).
and \( u \) at each iteration. Results are evaluated over each unlabeled set using the accuracy (ACC) and the standard F1 measure (F1) \[\text{Baeza-Yates and Ribeiro-Neto, 1999}\], which is the harmonic average of precision and recall. Reported performances are averaged over the 20 trials.

Table 2 summarizes results obtained by RF, FSLA, LP, OVA-TSVM and MSLA. We used bold face to indicate the highest performance rates and the symbol ↓ indicates that the performance is significantly worse than the best result, according to Mann-Whitney U test \[\text{Mann and Whitney, 1947}\] used at the p-value threshold of 0.01. From these results it comes out that

- compared to the fully supervised approach, RF, unlabeled training data may degrade performance in some cases. This may be due to the fact that the learning hypotheses of the learning algorithms are not met regarding the data sets where the decrease is observed;

- LP and OVA-TSVM did not pass the scale over larger data sets (SensIT and MNIST).

- Self-training approaches are more robust to the large-scale problem and MSLA provides significantly better results than other approaches on Pendigits, SensIT and MNIST.

- On DNA, with a very few number of labeled training examples, OVA-TSVM outperforms MSLA.

Our analysis of these results is that the self-training algorithm does better pass the scale but it is extremely sensitive to the choice of the initial classifier and the threshold used for pseudo-labeling. On DNA the number of labeled examples is too small, leading to a bad initialization of the first classifier trained over the labeled training set. The poor estimation of the margin \( m_Q(x, y) \) leads to a bad approximation of the conditional probability \( P(y|x) \) used in pseudo-labeling. On SensIT, Pendigits and MNIST collections (especially the two last), the initial RF classifier is efficient, but compared to FSLA, it comes out that the choice of the threshold for pseudo-labeling is crucial, and that using the conditional Bayes error rate, the margin of observations are good indicators to find such efficient thresholds. In the case of MNIST, the increase in performance compared to RF is about 4% on both the accuracy and the F1 measure.

We also analyze the behavior of the various algorithms for growing initial amounts of labeled data in the training set. Figure 1 illustrates this by showing the accuracy on a subsample of 3500 observations on MNIST of RF, FSLA\(\theta=0.7\) and MSLA with respect to the percentage of the labeled training examples. As expected, all performance curves increase monotonically with respect to the additional labeled data. When there are sufficient labeled training examples, all algorithms actually converge to the same accuracy performance, suggesting that the labeled data carries out sufficient information and no additional information could be extracted from unlabeled examples.

For a low number of labeled training data, the contribution of FSLA\(\theta=0.7\) and MSLA that use unlabeled data is clearly shown. Even when the initial supervised RF classifier is
efficient, an inexact threshold used for pseudo-labeling will lead to an addition of extra noise, making that the Random Forest trained over the augmented noisy data set becomes less effective than RF itself.

5 Conclusion

In this paper we proposed a bound over the transductive risk of a multi-class voted majority classifier. We showed how the bound can be obtained by considering the class confusion matrix as an error indicator, by involving the margin distribution of the classifier over each class and a bound over the risk of the associated Gibbs classifier. From our study, it came out that when the latter bound is tight and the errors of the majority vote classifier per class are concentrated on a low margin zone, the bound over the risk of the Bayes classifier is tight. We further showed that this bound can be solved analytically using a linear program. From this result, we then proposed to extend the self-training algorithm to the multi-class case by automatically finding a threshold for which the risk of the majority vote is the lowest. We provided empirical evidence of the extended algorithm compared to the case where the threshold is fixed manually, to a graph based semi-supervised approach and to the one-vs-all extension of TSVM. From the numerical results, it came out that the self-learning algorithm can better pass the scale but it is highly sensitive to the choice of the initial classifier trained over the labeled training set and to the threshold upon which unlabeled examples are pseudo-labeled. These results suggest that, considering the margin is effectively interesting.
6 Acknowledgments

Financial support was provided by a CNRS project PEPS and by IRS Grant (University Grenoble Alpes).

References


Dua Dheeru and Efi Karra Taniskidou. UCI machine learning repository, 2017.

