A Direct Boosting Approach for Semi-Supervised Classification

Shaodan Zhai, Tian Xia, Zhongliang Li, Shaojun Wang
Kno.e.sis Center
Wright State University, Dayton, US
{zhai.6,xia.7,li.141,shaojun.wang}@wright.edu

Abstract
We introduce a semi-supervised boosting approach (SSDBoost), which directly minimizes the classification errors and maximizes the margins on both labeled and unlabeled samples, without resorting to any upper bounds or approximations. A two-step algorithm based on coordinate descent/ascent is proposed to implement SSDBoost. Experiments on a number of UCI datasets and synthetic data show that SSDBoost gives competitive or superior results over the state-of-the-art supervised and semi-supervised boosting algorithms in the cases that the labeled data is limited, and it is very robust in noisy cases.

1 Introduction
In many applications of classifiers, labeled data is usually limited while unlabeled data can often be much cheaper and more plentiful than labeled data. Semi-supervised learning is a way to employ a large amount of unlabeled data together with a few labeled data to construct a classifier with good generalization.

Boosting, as an ensemble learning framework, is one of the most powerful classification algorithms in supervised learning. Based on the gradient descent view of boosting [Mason et al., 2000], many semi-supervised boosting methods have been proposed, such as SMarginBoost [d’Alché-Buc et al., 2002], ASSEMBLE [Bennett et al., 2002], RegBoost [Chen and Wang, 2007; Chen and Wang, 2011], SemiBoost [Mallapragada et al., 2009], SERBoost [Saffari et al., 2008] and information theoretic regularization based boosting [Zheng et al., 2009], where a margin loss function is minimized over both labeled and unlabeled data by the functional gradient descent method. The effectiveness of these methods can be ascribed to their tendency to produce large margin classifiers with a small classification error. However, these algorithms were not designed to directly maximize the margin (although some of them have the effects of margin enforcing), and the objective functions are not related to the margin in the sense that one can minimize these loss functions while simultaneously achieving a bad margin [Rudin et al., 2004]. Therefore, a natural goal is to construct classifiers that directly optimize margins as measured on both labeled and unlabeled data.

In this paper, we propose a new semi-supervised direct boosting method named SSDBoost that extends the work of DirectBoost [Zhai et al., 2013] to semi-supervised classification. The process of SSDBoost includes two steps: it first directly minimizes a generalized classification error that extends the concept of classification error to both labeled and unlabeled data, by iteratively adding base classifiers to the ensemble classifier. Once the generalized classification error reaches a coordinate-wise local minimum1, it continuously adds base classifiers by directly maximizing a generalized average margin that consists of both labeled and unlabeled margins. The first step serves as an initialization method of the second step, the motivation is that the margin maximization algorithm often performs better when it starts with a low classification error.

Both SSDBoost and DirectBoost [Zhai et al., 2013] are coordinate optimizations in the hypothesis space, where only one coordinate is chosen and the corresponding parameter is updated at each iteration. However, SSDBoost is a non-trivial extension of DirectBoost to semi-supervised classification, where we have to mathematically re-formulated the semi-supervised boosting approach by extending the classification error and margin function to unlabeled data. Since the objectives in SSDBoost are more complicated, we designed new optimization techniques and provide the rationales behind our approach. We will show that SSDBoost is able to exploit easily-obtained unlabeled data to significantly improve accuracy, especially in the noisy cases. Due to space limitation, the proofs of properties and theorem are given in the supplementary material.

2 SSDBoost Algorithm
Let $\mathcal{H} = \{h_1, ..., h_{|\mathcal{H}|}\}$ denote the set of all possible weak classifiers that can be produced by the weak learning algorithm, where a weak classifier $h_j \in \mathcal{H}$ is a mapping from an instance space $\mathcal{X}$ to $\mathcal{Y} = \{-1, 1\}$, and $\mathcal{H}$ is closed under negation, i.e., both $h$ and $-h$ belong to $\mathcal{H}$. In this study, we use decision trees as the weak learning algorithm2, then $|\mathcal{H}|$ is finite but can be extremely large.

1See the definition on page 479 in [Tseng, 2001].
2As the combination of boosting with decision trees is the state-of-the-art approach [Appel et al., 2013].
Assume we are provided \( n \) labeled samples, \( D^l = \{(x_1,y_1), \cdots , (x_n,y_n)\} \) and \( m \) unlabeled samples, \( D^u = \{x_{n+1}, \cdots , x_N\} \) (let \( N = n + m \)). Semi-supervised boosting combines weak classifiers to form a highly accurate ensemble classifier by using the combined training set \( D = D^l \cup D^u \). Formally, for binary classification, the ensemble classifier is defined to be \( \text{sign}(f(x)) \), where \( f(x) = \sum_{h \in H} \alpha_h b_h(x) \), \( \alpha_h \geq 0 \) is the ensemble function. Our goal is to find an ensemble classifier that has good generalization performance. To this end, we developed a semi-supervised boosting approach through two steps. In the following, we will elaborate the two steps respectively.

2.1 Minimize generalized classification error

For the labeled data, the classification error (or 0-1 loss) is defined to be

\[
\text{error}(f, D^l) = \frac{1}{n} \sum_{i=1}^{n} 1(y_i f(x_i) \leq 0)
\]  

(1)

where \( 1(\cdot) \) is an indicator function. While optimizing the classification error is NP-hard, it is robust to noise [Nguyen and Sanner, 2013] and is consistent under certain conditions [Vapnik, 1998]. For \( D^u \), since the labels are unknown, a natural extension of the 0-1 loss is the expected classification error

\[
\text{error}(f, D^u) = \frac{1}{m} \sum_{i=n+1}^{N} \sum_{y \in Y} p(y|x_i) 1(y f(x_i) \leq 0)
\]

(2)

Minimizing (2) has the effects to push \( p(y|x) \) away from 0.5, so that the uncertainty of the putative labels is reduced. For binary classification tasks, the logistic (sigmoid) function of \( y f(x) \), \( \text{sigmoid}(y f(x_i)) = 1/(1 + \exp(-y f(x_i))) \), is a good estimation of \( p(y|x) \) [Schapire and Freund, 2012], and then the loss of the minimum entropy semi-supervised boosting method [Zheng et al., 2009] is a surrogate upper bound of (2). Combining (1) and (2), we have the generalized classification error

\[
\text{error}(f, D) = \text{error}(f, D^l) + \gamma \text{error}(f, D^u)
\]

(3)

where \( \gamma \) is a trade-off parameter that controls the influence of the unlabeled data.

Consider the \( t \)th iteration, the ensemble function is

\[
f_t(x) = \sum_{k=1}^{t} \alpha_k h_k(x) + \alpha_t h_t(x)
\]

(4)

where previous \( t - 1 \) weak classifiers \( h_k(x) \) and corresponding weights \( \alpha_k, k = 1, \cdots , t - 1 \) have been selected and determined. Then for a new weak classifier \( h_t(x) \), the goal is to choose its weight \( \alpha_t \) such that (3) is minimized. If we estimate \( p(y|x) \) by \( \text{sigmoid}(y f(x_i)) \), the second term of (3) is a complex function of \( \alpha_t \), and thus it is difficult to compute the optimal \( \alpha_t \). Instead, we estimate \( p(y|x) \) by the logistic function of \( f \) of the previous step, \( \text{sigmoid}(y f_{t-1}(x_i)) \), and update the estimation through an iterative scheme. We define \( \text{error}(f, D^u) \) to be

\[
\frac{1}{m} \sum_{i=n+1}^{N} \sum_{y \in Y} \hat{p}(y|x_i) 1(y f(x_i) \leq 0)
\]

Algorithm 1 Minimize the generalized 0-1 loss on \( D \).

1: Initialize: \( t = 0, f_t(x_i) = 0, i = 1, \cdots , N \).
2: repeat
3: \( t \leftarrow t + 1 \).
4: \( \hat{p}(y|x_i) = \text{sigmoid}(y f_{t-1}(x_i)) \) for \( x_i \in D^u \).
5: Sort \( \{f_{t-1}(x_i)\}, x_i \in D \) in an increasing order.
6: Pick a weak classifier \( h_t \) by Algorithm 1-2.
7: Get the interval that has the minimum value of (5) by calling Algorithm 1-1 with \( h_t \), and set \( \alpha_t \) to be the value within this interval.
8: Update: \( f_t(x_i) = f_{t-1}(x_i) + \alpha_t h_t(x_i) \).
9: until (5) reaches a local coordinate minimum.
10: Output: \( f_t(x_i) \).

Algorithm 1-1 Line search algorithm to find the interval with the minimum generalized 0-1 loss.

1: Input: a weak classifier \( h_t \in H \).
2: for \( i = 1, \cdots , N \) do
3: Compute the value of (5) at \( \alpha_t = 0 \).
4: Let \( e_i = |f_{t-1}(x_i)| \).
5: if \( (\text{slope} > 0 \text{ and intercept} < 0) \), then error update on the righthand side of \( \varepsilon_i = -\frac{1}{n} \) for \( x_i \in D^l \) or \( -\frac{\hat{p}(y f_t + 1 | x_i) - \hat{p}(y f_t - 1 | x_i)}{m} \) for \( x_i \in D^u \).
6: if \( (\text{slope} < 0 \text{ and intercept} > 0) \), then error update on the righthand side of \( \varepsilon_i = \frac{1}{n} \) for \( x_i \in D^l \) or \( \frac{\hat{p}(y f_t + 1 | x_i) - \hat{p}(y f_t - 1 | x_i)}{m} \) for \( x_i \in D^u \).
7: end for
8: Incrementally calculate (5) on intervals of \( \varepsilon_i \)’s.
9: Output: the interval with minimum generalized 0-1 loss.

by replacing \( p(y|x_i) \) in \( \text{error}(f, D^u) \) by \( \hat{p}(y|x_i) \). Therefore, the estimation of (3) is to be

\[
\text{error}(f, D) = \text{error}(f, D^l) + \gamma \text{error}(f, D^u)
\]

(5)

which is a stepwise function of \( \alpha_t \).

Algorithm 1 outlines a greedy coordinate descent algorithm to directly minimize (5). The line search algorithm, Algorithm 1-1, describes the way to find the optimal \( \alpha \) for any given hypothesis \( h \in H \) such that (5) is minimized. The key is how to efficiently find the points that lead (5) changes. Denoting the inference function of a sample \( x_i \) to be

\[
F_t(x_i, y) = y \hat{h}_t(x_i) \alpha_t + y f_{t-1}(x_i)
\]

(6)

which is a linear function with slope \( \gamma h_t(x_i) \) and intercept \( y f_{t-1}(x_i) \). For a labeled sample \( (x_i, y_i) \), \( F_t(x_i, y_i) > 0 \) indicates this sample is correctly classified; otherwise, it is misclassified. These two states exchange at the point \( \alpha_t = -\frac{1}{h_t(x_i)} \), we denote this point as a critical point \( e_i \). Thus, the value of the generalized 0-1 loss (5) has \( \frac{1}{n} \) differences at \( e_i \). To compute the “classification error” of an unlabeled sample, we use \( \hat{y}_i = \text{sign}(f_{t-1}(x_i)) \) to denote its pseudo label. Similarly, the sign of \( F_t(x_i, \hat{y}_i) \) identifies \( x_i \in D^u \) is “correctly classified” or “misclassified”. Again, the critical point for \( x_i \in D^u \) is \( e_i = -\frac{1}{h_t(x_i)} \), and the value of (5) has
Algorithm 1-2 Weak learning algorithm.

1: **Input:** a training set \( D \), current tree depth \( \ell \).
2: if \( \ell \leq \text{max depth} \) then
3: for a binary split do
4: Split \( D \) into \( D_{\text{left}} \) and \( D_{\text{right}} \), then a weak hypothesis \( h \in H \) is generated which maps \( D_{\text{left}} \) to +1 and \( D_{\text{right}} \) to -1.
5: Call Algorithm 1-1 with \( D_{\text{left}} \) and \( D_{\text{right}} \) with an increasing order, the critical points are
6: end for
7: Choose the optimal binary split which partitions \( D \) into \( D_{\text{left}} \) and \( D_{\text{right}} \), update \( h_t \) with the corresponding labels on \( D_{\text{left}} \) and \( D_{\text{right}} \).
8: Call weak learning algorithm with \( D_{\text{left}} \) and \( \ell + 1 \).
9: Call weak learning algorithm with \( D_{\text{right}} \) and \( \ell + 1 \).
10: end if
11: **Output:** a weak classifier \( h_t \in H \).

none of them has been shown to maximize the margins on \( D^l \cup D^u \), although some of them employ margin enforcing loss functions. In this section, we introduce a generalized average margin on \( D^l \cup D^u \), and propose a coordinate ascent algorithm that directly maximizes this objective function.

The (normalized) margin of a labeled sample \( (x_i, y_i) \) w.r.t \( f_t(x_i) \) is defined to be \( \varphi^l_i = \frac{y_if(t)}{\sum_{k=1}^{n} \alpha_k} \), which can be interpreted as a measure of how confidently this labeled sample is correctly classified. For an unlabeled sample \( x_i \), it is natural to define its margin as the expected margin:

\[
\varphi^u_i = \frac{1}{n^l} \sum_{y \in Y}^{n^l} p(y|x_i) \frac{y_if(t)}{\sum_{k=1}^{n} \alpha_k}
\]

where \( B^l_i \) denotes the set of \( n^l \) labeled samples having the smallest margins, and \( B^u_i \) denotes the set of \( n^u \) unlabeled samples having the smallest margins. The parameter \( n^l \) indicates how much we relax the hard margin on labeled samples, and we often set \( n^l \) based on knowledge of the number of noisy samples in \( D^l \) [Ratsch et al., 2000]. The higher the noise rate, the larger the \( n^l \) should be used. The parameter \( n^u \) controls the relaxation of the margin distribution over the unlabeled data. A smaller \( n^u \) makes the algorithm focus more on the unlabeled samples close to the decision boundary.

For an unlabeled sample \( x_i \), again we estimate \( p(y|x_i) \) by \( \hat{p}(y|x_i) = \text{sigmoid}(yfi^{-1}(x_i)) \). Denote \( \hat{y}_i = \frac{1}{1 + e^{-(fi^{-1}(x_i))}} - 1 \), then the estimated margin of \( x_i \) is

\[
\varphi^u_i = \hat{y}_i - \frac{fi^{-1}(x_i) + \alpha_i h(t)}{\sum_{k=1}^{n^l} \alpha_k + \alpha_i}
\]

Thus, the objective function that we are working on in the margin maximization step is

\[
\varphi_{\text{avg}}(n',m') = \frac{1}{n^l'} \sum_{y \in B^l_i} \varphi^l_i + \frac{1}{m^l'} \sum_{x \in B^u_i} \varphi^u_i
\]

The outline of the greedy coordinate ascent algorithm that sequentially maximizes (10) is described in Algorithm 2. We first sort \( \varphi^l_i \) and \( \varphi^u_i \) in an increasing order respectively, and consider \( n^l \) worst labeled samples \( n^l \leq n \) and \( n^u \) worst unlabeled samples \( n^u \leq m \) that have smaller margins, then the generalized average margin over those samples is

\[
\hat{\phi}_{\text{avg}}(n',m') = \frac{1}{n^l} \sum_{i \in B^l_i} \varphi^l_i + \frac{1}{m^l} \sum_{i \in B^u_i} \varphi^u_i
\]

1Decision stumps are the decision trees with a depth of 1. The computational costs of Algorithm 1 has the same increasing rate as the methods in [Bennett et al., 2002; Zheng et al., 2009], except that large trees are considered.
Algorithms 1 and 2 are not shown in this text. Instead, here's a reformatted version of the content:

**Algorithm 2** Maximize margins on $D^i \cup D^u$.

1. Initialize: $t$ and $f_t$ from Algorithm 1.
2. repeat
3. $t \leftarrow t + 1$.
4. Update $\hat{y}_i = \frac{-2}{1 + e^{-f_t(x_i)}} - 1$, $i = n + 1, \ldots, N$.
5. Sort $\hat{\phi}^{-1} = \hat{\phi}^{-1}_i, \ldots, \hat{\phi}^{-1}_N$ and $\hat{\phi}^u = \hat{\phi}^u_i, \ldots, \hat{\phi}^u_N$ in increasing order at $\alpha_t = 0$ respectively, determine $B^i_t$, and $B^u_t$.
6. Pick a weak classifier $h_t$ by weak learning algorithm.
7. Compute $q_t$ by Algorithm 2-1 that maximizes (10) along the coordinate $h_t$. Set $\alpha_t = q_t$.
8. Update $f_t(x_i) = f_{t-1}(x_i) + \alpha_t h_t(x_i)$.
9. until $\hat{\phi}_{\text{avg}}(h', m')$ reaches a local coordinate wise maximum.
10. Output: $f_t(x_i)$.

Since $c \geq y_i f_{t-1}(x_i)$, depending on the sign of $y_i h_t(x_i)$, (11) is either positive or negative, which is irrelevant to the value of $\alpha_t$. That is, if the labeled sample $(x_i, y_i) \in D^i$ is correctly classified by $h_t$ ($h_t(x_i) > 0$), then $\hat{\phi}_i$ is monotonically increasing with respect to $\alpha_t$. Otherwise, $\hat{\phi}_i$ is monotonically decreasing. Similarly, for an unlabeled sample $x_i$, the derivative of $\hat{\phi}_i$ is either positive or negative depending on the sign of $y_i h_t(x_i)$, and which is irrelevant to the value of $\alpha_t$. Hence for an interval of $\alpha_t$ with the fixed $B^{i'}_u$ and $B^{u'}_m$, the derivative of (10) is

$$
\frac{\partial \hat{\phi}_{\text{avg}}(n', m', \alpha_t)}{\partial \alpha_t} = \frac{1}{m'} \sum_{i \in B^{i'}_u} y_i (h_t(x_i) c_{t-1} - f_{t-1}(x_i)) (c_{t-1} + \alpha_t)^2 + \frac{1}{m'} \sum_{i \in B^{u'}_m} y_i (h_t(x_i) c_{t-1} - f_{t-1}(x_i)) (c_{t-1} + \alpha_t)^2
$$

which sign is irrelevant to the value of $\alpha_t$. Thus, with the fixed $B^{i'}_u$ and $B^{u'}_m$, $\hat{\phi}_{\text{avg}}(n', m', \alpha_t)$ is a monotonic function of $\alpha_t$, depending on the sign of the derivative in (12), it is maximized either on the left side or on the right side of the interval.

Along the $h_t$ coordinate, $B^{i'}_u$ and $B^{u'}_m$ are not always fixed, hence we need to check the values of $\alpha_t$ that lead $B^{i'}_u$, or $B^{u'}_m$, to change. To address this, we first examine when the margins $\hat{\phi}_i$ and $\hat{\phi}_j$ of two labeled samples $(x_i, y_i)$ and $(x_j, y_j)$ intersect. Since $H$ is closed under negation, it is not necessary to consider the cases that their intersection is negative. Obviously $\hat{\phi}_i$ and $\hat{\phi}_j$ never intersect when they are both increasing or decreasing. Otherwise, $\hat{\phi}_i$ and $\hat{\phi}_j$ intersect with each other at

$$
\alpha_t = \frac{y_j f_{t-1}(x_i) - y_i f_{t-1}(x_i)}{y_j h_t(x_i) - y_i h_t(x_j)}
$$

As $\hat{\phi}_i$’s are sorted in advance (Algorithm 2, line 5), we can compute the intersections that result in the change of $B^{i'}_u$, very efficiently by Property 1.

**Property 1** All the points that lead $B^{i'}_u$ to change can be determined by computing the intersections of the $j$th highest increasing margin in $B^{i'}_u$ and $j$th smallest decreasing margin in the complementary set of $B^{i'}_u$.

---

**Proof:** Let $\hat{\phi}_i^{inc}$ denotes the $j$th highest increasing margin in $B^{i'}_u$ at $\alpha_t = 0$, and $\hat{\phi}_i^{dec}$ denotes the $j$th smallest decreasing margin in $(B^{i'}_u)^c$ at $\alpha_t = 0$. Denoting $q_j$ to be the intersection of $(\hat{\phi}_i^{inc})$ and $(\hat{\phi}_i^{dec})$.

For $j = 1$, it is obviously that $(\hat{\phi}_i^{dec})$ is the first margin in $(B^{i'}_u)^c$ that intersects with $(\hat{\phi}_i^{inc})$. Therefore, $q_1$ leads $B^{i'}_u$ to change as $(\hat{\phi}_i^{dec})$ belongs to $B^{i'}_u$ and $(\hat{\phi}_i^{inc})$ belongs to $(B^{i'}_u)^c$ on the right side of $q_1$.

Suppose the conclusion holds for $j = k - 1$. For $j = k$, since $(\hat{\phi}_i^{dec})$, $(\hat{\phi}_i^{dec})$ belong to $B^{i'}_u$, the intersections of $(\hat{\phi}_i^{inc})$ and those margins do not lead $B^{i'}_u$ to change. Hence $(\hat{\phi}_i^{inc})$ is the first margin in $(B^{i'}_u)^c$ that intersects with $(\hat{\phi}_i^{inc})$, and the intersection $q_k$ leads $B^{i'}_u$ to change.

In addition, the following properties indicate that we do not need to consider the cases that the margins of two unlabeled data are both increasing or decreasing.

**Property 2** If $\hat{\phi}_i$ and $\hat{\phi}_j$ are both increasing, then they never intersect when $\alpha_t > 0$.

**Proof:** For any unlabeled sample $x \in D^u$, $y = \frac{1}{1 + e^{-f_{t-1}(x)}} - 1$ is a strictly monotonic function with $f_{t-1}(x)$, and $f_{t-1}(x)\hat{y} \geq 0$ always holds.

Without loss of generality, we assume $f_{t-1}(x) > f_{t-1}(x)$, then $y f_{t-1}(x) - y f_{t-1}(x) < 0$. Since $\hat{\phi}_i$ and $\hat{\phi}_j$ are both increasing, we have $h_t(x_i)f_{t-1}(x_i) > 0$, $h_t(x_j)f_{t-1}(x_j) > 0$, and $h_t(x_i)\hat{y}_i > h_t(x_j)\hat{y}_j > 0$. Thus

$$
\frac{\hat{y}_j f_{t-1}(x) - \hat{y}_i f_{t-1}(x)}{h_t(x_i)\hat{y}_i - h_t(x_j)\hat{y}_j} < 0.
$$

That indicates $\hat{\phi}_i$ intersects $\hat{\phi}_j$ at $\alpha_t < 0$.

**Property 3** If $\hat{\phi}_i$ and $\hat{\phi}_j$ are both decreasing, then they only intersect each other after intersecting with all the increasing margins.

**Proof:** For any decreasing margins $\hat{\phi}_i$ and $\hat{\phi}_j$ in $(B^{i'}_u)^c$, and any increasing margin $\hat{\phi}_k$ in $B^{i'}_u$, if we assume $\hat{\phi}_k$ intersects $\hat{\phi}_i$ at $q_{i,k}$, $\hat{\phi}_k$ intersects $\hat{\phi}_j$ at $q_{i,j}$, and $\hat{\phi}_i$ intersects $\hat{\phi}_j$ at $q_{i,j}$, it is suffices to show $q_{i,j} > q_{i,k}$ and $q_{i,j} > q_{j,k}$.

Since $\hat{\phi}_i > \hat{\phi}_k$ and $\hat{\phi}_j > \hat{\phi}_k$, then $f_{t-1}(x) > f_{t-1}(x)$. Thus we have

$$
q_{i,k} = \frac{\hat{y}_i f_{t-1}(x_i) - \hat{y}_i f_{t-1}(x_i)}{h_t(x_i)\hat{y}_i - h_t(x_i)\hat{y}_j}
$$

We can prove the case $q_{i,k} < q_{i,j}$ in the same way.

Thus, the points that lead $B^{i'}_u$ to change can be computed in the similar way as described in Property 1.

Based on the above discussion, we are able to efficiently compute all the intersections that lead $B^{i'}_u$ or $B^{u'}_m$ to change.
We now prove that $S_{cave}$ on $S$ set. By definition of quasiconcave, margins are smallest for a fixed $\alpha$ and we have to compute (10) for each of them. Fortunately, we can prove that (10) is a quasi-concave function for any given weak hypothesis (in Theorem 1), that allows us to determine $q^*$ by incrementally updating (12) and checking its sign in $O(n' + m')$. Specifically, if $\frac{\partial \phi_{avg}(n', m')}{\partial q_i} > 0$ and $\frac{\partial \phi_{avg}(n', m')}{\partial q_{i+1}} < 0$, then $q^* = q_j$.

Theorem 1 Denote the average margin of the bottom $n'$ labeled samples and $m'$ unlabeled samples as

$$\phi_{avg}(n', m')(\alpha_t) = \frac{1}{n'} \sum_{i \in \{B_{n'}^{+}\} \alpha_t} \varphi_i^t + \frac{1}{m'} \sum_{i \in \{B_{m'}^{+}\} \alpha_t} \varphi_i^u$$

where $\{B_{n'}^{+}\} \alpha_t$ denotes the set of $n'$ labeled samples whose margins are smallest for a fixed $\alpha_t$, and $\{B_{m'}^{+}\} \alpha_t$ denotes the set of $m'$ unlabeled samples whose margins are smallest for a fixed $\alpha_t$. Then $\phi_{avg}(n', m')(\alpha_t)$ is quasiconcave.

Proof (outline) : Let $S = \{\alpha_t : \alpha_t > 0\}$, which is a convex set. By definition of quasiconcave, $\phi_{avg}(n', m')(\alpha_t)$ is quasiconcave on $S$ if and only if its upper contour sets are convex sets on $S$. The $\mu$-upper-contour set $S_\mu$ of $\phi_{avg}(n', m')(\alpha_t)$ on $S$ is denoted as

$$S_\mu = \{\alpha_t : \alpha_t > 0, \phi_{avg}(n', m')(\alpha_t) \geq \mu\}$$

We now prove that $S_\mu$ is a convex set. For $\forall \alpha_t^{(1)}, \alpha_t^{(2)} \in S_\mu$ and $\forall \lambda \in [0, 1]$, letting $\theta = (1 - \lambda)\alpha_t^{(1)} + \lambda\alpha_t^{(2)}$ then we have

$$\min \left\{ \frac{1}{n'} \sum_{i \in \{B_{n'}^{+}\} \alpha_t} \varphi_i^t(x_i) + \theta \varphi_i^t(x_i) \right\} + \min \left\{ \frac{1}{m'} \sum_{i \in \{B_{m'}^{+}\} \alpha_t} \varphi_i^u(x_i) + \theta \varphi_i^u(x_i) \right\}$$

$$
\geq (1 - \lambda)\mu(\sum_{k=1}^{t-1} \alpha_k + \alpha_t^{(1)}) + \lambda\mu(\sum_{k=1}^{t-1} \alpha_k + \alpha_t^{(2)})$$

$$\geq \mu(\sum_{k=1}^{t-1} \alpha_k + \theta)$$

Therefore, $\theta \in S_\mu$, $\phi_{avg}(n', m')(\alpha_t)$ is quasiconcave.

Formally, the line search algorithm to calculate the value of $q^*$ is described in Algorithm 2-1. The way to select the weak classifier is very similar to Algorithm 1-2, the only modification is to replace the line search algorithm to Algorithm 2-1. Since $\phi_{avg}(n', m')$ is bounded, apparently Algorithm 2 converges to a coordinatewise local maximum. If there are $L$ possible binary splits, the computational cost of Algorithm 2 is $O(L(n' + m') + N \log N)$ on each round.

Since $\phi_{avg}(n', m')$ is non-differentiable at the intersections, the coordinate ascent algorithm may get stuck at a corner from which it is impossible to make progress along any coordinate direction. To overcome this difficulty, we employ an $\epsilon$-relaxation method [Bertsekas, 1998]. The main idea is to allow a single coordinate to change even if this worsens the objective function. When a coordinate is changed, however, it is set to $\epsilon$ plus the value that maximizes the margin function along that coordinate, where $\epsilon$ is a positive number. If $\epsilon$ is small enough, the algorithm can eventually approach a small neighborhood of the optimal solution.

3 Experiments

In this section, we first evaluate the performance of SSDBoost on 10 UCI datasets from the UCI repository [Frank and Asuncion, 2010], then examine its noise robustness on two datasets with random label noise. For comparison, we also report the results of several existing supervised boosting methods (AdaBoost [Freund and Schapire, 1997], LPBoost [Demiriz et al., 2002], and DirectBoost [Zhai et al., 2013]) and semi-supervised boosting methods (ASSEMBLE [Bennett et al., 2002] and semi-supervised entropy regularized boosting [Zheng et al., 2009] (denoted as SERBoost)). For all the algorithms in the comparison, we use decision trees as the weak learners. Note that it is not our intention to show
that the proposed algorithm always outperforms a variety of supervised and semi-supervised learning methods. Instead, the empirical study is focused on whether the proposed SSDBoost is able to effectively improve the accuracy of the well-known boosting algorithms with the same weak hypothesis space \( \mathcal{H} \). Thus, same as the ways the authors did in [Bennett et al., 2002; Chen and Wang, 2007; Demiriz et al., 2002; Zheng et al., 2009], we restrict the comparison with only boosting methods and the same weak learning algorithm, rather than other related works, such as Semi-Supervised Support Vector Machines (S3VM) [Chapelle et al., 2006; Joachims, 1999; Sindhwani et al., 2006].

The classification error is estimated by 10-fold cross-validation. For each dataset, we partition it into 10 parts evenly. In each fold, we use eight parts for training, one part for validation, and the remaining part for testing. Within the eight parts of training data, only one part is used as labeled data, and the other parts are treated as unlabeled data (by simply discarding the labels). Since we concentrate on the cases where the labeled data are limited while the unlabeled data are adequate in the training process, the datasets we selected include datasets of small or moderate sizes, and only a small part (one tenth) is used as labeled data.

### 3.1 UCI datasets

Table 1 shows, as we expected, the semi-supervised boosting algorithms (ASSEMBLE, EntropyBoost, and SSDBoost) outperform the supervised methods (AdaBoost, LPBoost, and DirectBoost) in general, the results indicate that the unlabeled data does help to improve generalization performance. By taking advantage of maximizing margins directly on both labeled and unlabeled data, SSDBoost gives the most accurate results (highlighted in bold font) in 7 of the 10 datasets among all the methods, and its results are close to the best results produced by the other methods for the remaining 3 datasets. We have also performed a significance test using the paired t-test. When compared to AdaBoost, SSDBoost has statistically significant improvements (p-value is less than 0.05) on Australian, Splice, and WPBC datasets.

We noticed that for some moderate size of datasets (such as Adult, Mushroom, and Kr-vs-Kp), the semi-supervised boosting methods do not provide much improvements. We believe the reason that there was little improvement for those datasets is that the numbers of labeled samples are enough to get reasonable results, so there is little room in the classification to improve accuracy further. We selected two datasets, Kr-vs-kp and Mushrooms, and we tried to reduce their size in order to show the power of semi-supervised learning. Table 2 shows the results of Kr-vs-kp and Mushroom datasets with 50 and 20 labeled samples respectively. When the labeled data is extremely limited, semi-supervised methods show their advantage more clearly, and SSDBoost is very efficient at utilizing the information of unlabeled data.

---

Table 1: # of samples (\( M \)), # of attributes (\( D \)), mean error rates (in %) and standard deviations of boosting methods on 10 UCI datasets.

<table>
<thead>
<tr>
<th>Data</th>
<th>( M )</th>
<th>( D )</th>
<th>AdaBoost</th>
<th>LPBoost</th>
<th>DirectBoost</th>
<th>ASSEMBLE</th>
<th>EntropyBoost</th>
<th>SSDBoost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult</td>
<td>48842</td>
<td>14</td>
<td>33.33 (5.2)</td>
<td>32.22 (6.6)</td>
<td>31.11 (5.6)</td>
<td>17.83 (2.7)</td>
<td>17.83 (2.5)</td>
<td>16.38 (2.5)</td>
</tr>
<tr>
<td>Australian</td>
<td>690</td>
<td>14</td>
<td>17.83 (2.7)</td>
<td>17.83 (2.5)</td>
<td>3.98 (1.9)</td>
<td>9.7 (1.8)</td>
<td>7.38 (1.8)</td>
<td>5.05 (0.7)</td>
</tr>
<tr>
<td>Kr-vs-kp</td>
<td>3196</td>
<td>36</td>
<td>3.98 (1.8)</td>
<td>4.01 (1.2)</td>
<td>3.89 (0.9)</td>
<td>3.45 (1.1)</td>
<td>3.39 (1.4)</td>
<td>3.39 (0.5)</td>
</tr>
<tr>
<td>Liver</td>
<td>345</td>
<td>7</td>
<td>36.76 (3.4)</td>
<td>38.53 (4.9)</td>
<td>36.65 (4.4)</td>
<td>36.18 (3.7)</td>
<td>36.35 (4.9)</td>
<td>33.24 (7.3)</td>
</tr>
<tr>
<td>Mushroom</td>
<td>8124</td>
<td>22</td>
<td>0.1 (0.1)</td>
<td>0.9 (0.5)</td>
<td>0.18 (0.2)</td>
<td>0.11 (0.1)</td>
<td>0.12 (0.1)</td>
<td>0.16 (0.2)</td>
</tr>
<tr>
<td>Sonar</td>
<td>208</td>
<td>60</td>
<td>33.33 (5.2)</td>
<td>32.22 (6.6)</td>
<td>31.11 (5.6)</td>
<td>28.33 (3.6)</td>
<td>28.89 (4.1)</td>
<td>28.44 (5.2)</td>
</tr>
<tr>
<td>Spambase</td>
<td>4601</td>
<td>57</td>
<td>7.5 (0.9)</td>
<td>7.52 (0.8)</td>
<td>7.35 (1.1)</td>
<td>7.48 (0.7)</td>
<td>7.87 (0.9)</td>
<td>7.09 (1.4)</td>
</tr>
<tr>
<td>Splice</td>
<td>3190</td>
<td>61</td>
<td>14.6 (2.7)</td>
<td>15.3 (2.2)</td>
<td>14.6 (2.8)</td>
<td>14.8 (2.7)</td>
<td>14.9 (2.7)</td>
<td>12.0 (1.7)</td>
</tr>
<tr>
<td>WDBC</td>
<td>569</td>
<td>31</td>
<td>6.55 (1.6)</td>
<td>6.94 (1.9)</td>
<td>6.94 (1.8)</td>
<td>7.54 (2.1)</td>
<td>7.73 (2.1)</td>
<td>6.15 (1.8)</td>
</tr>
<tr>
<td>WPBC</td>
<td>198</td>
<td>34</td>
<td>33.68 (4.8)</td>
<td>34.21 (6.0)</td>
<td>32.63 (3.7)</td>
<td>28.95 (4.4)</td>
<td>29.68 (5.7)</td>
<td>28.95 (3.8)</td>
</tr>
</tbody>
</table>

Table 2: Mean error rates (in %) and standard deviations of boosting methods on Kr-vs-Kp (with 50 labeled samples) and Mushroom (with 20 labeled samples) datasets.

<table>
<thead>
<tr>
<th>Data</th>
<th>AdaBoost</th>
<th>LPBoost</th>
<th>DirectBoost</th>
<th>ASSEMBLE</th>
<th>EntropyBoost</th>
<th>SSDBoost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kr-vs-kp (50)</td>
<td>10.46 (2.2)</td>
<td>9.9 (2.4)</td>
<td>9.66 (2.4)</td>
<td>8.2 (2.2)</td>
<td>8.5 (2.1)</td>
<td>7.65 (2.0)</td>
</tr>
<tr>
<td>Mushroom (20)</td>
<td>8.81 (1.9)</td>
<td>9.7 (1.8)</td>
<td>7.38 (1.8)</td>
<td>5.05 (0.7)</td>
<td>5.1 (1.6)</td>
<td>2.2 (0.5)</td>
</tr>
<tr>
<td>Data</td>
<td>$\eta$</td>
<td>AdaBoost</td>
<td>LPBoost</td>
<td>DirectBoost</td>
<td>ASSEMBLE</td>
<td>EntropyBoost</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td>----------</td>
<td>---------</td>
<td>-------------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>Synthetic</td>
<td>0</td>
<td>13.12(1.6)</td>
<td>13.96(1.7)</td>
<td>12.6(1.2)</td>
<td>12.28(2.5)</td>
<td>11.8(1.0)</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>19.52(3.9)</td>
<td>19.36(4.9)</td>
<td>16.56(3.7)</td>
<td>16.92(2.7)</td>
<td>17.88(3.9)</td>
</tr>
<tr>
<td></td>
<td>0.2</td>
<td>29.08(3.1)</td>
<td>22.84(5.4)</td>
<td>22.12(4.6)</td>
<td>25.68(3.1)</td>
<td>25.52(5.5)</td>
</tr>
<tr>
<td>Kr-vs-Kp</td>
<td>0</td>
<td>10.42(2.2)</td>
<td>9.96(3.1)</td>
<td>10.08(4.1)</td>
<td>8.2(2.8)</td>
<td>8.36(2.6)</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>18.26(5.1)</td>
<td>18.09(4.9)</td>
<td>17.17(7.9)</td>
<td>16.66(5.8)</td>
<td>17.14(7.0)</td>
</tr>
<tr>
<td></td>
<td>0.2</td>
<td>27.18(8.3)</td>
<td>25.58(7.2)</td>
<td>22.46(7.7)</td>
<td>20.84(7.7)</td>
<td>21.4(7.5)</td>
</tr>
</tbody>
</table>

Table 3: Mean error rates (in %) and standard deviations of each boosting algorithm on synthetic and Kr-vs-Kp data with a label noise rate $\eta$ at 0%, 5%, and 20%.

3.2 Evaluation of Noise Robustness

In many real-world applications, robustness of a classifier is quite desirable. In this section, we run each boosting algorithm on the datasets with additional random label noise. We first use synthetic data with 5 real valued features which are generated by the model introduced in [Mease and Wyner, 2008]. In the experiments, we let the number of labeled, unlabeled training, validation and testing data be 50, 500, 500 respectively, and the labels of the labeled training data are corrupted with a noise rate $\eta$ at 0%, 5% and 20%. The experiments are repeated 10 times. In addition, we use Kr-vs-Kp dataset again, but this time we flip the labels of the labeled training data by a noise rate $\eta$. Table 3 shows the results of each boosting algorithm. Similar to AdaBoost, ASSEMBLE and EntropyBoost are very sensitive to noise [Long and Servedio, 2010], their accuracy is hurt even with a 5% noise rate. In contrast, the algorithms that maximize the average bottom samples (including LPBoost, DirectBoost, and SSDBoost) perform much better on the noisy cases. Particularly, SSDBoost does very well by utilizing the unlabeled data.

Figure 2 shows the cumulative margin distributions on $D^l$ and $D^u$ respectively of semi-supervised boosting methods on the synthetic data with 20% label noise, where the margins of unlabeled data are measured in (8). For the margin distribution of labeled samples, as shown in the left panel, ASSEMBLE and EntropyBoost concentrate their resources on a few difficult samples, but these samples are usually noisy. SSDBoost allows some misclassifications to achieve a better margin distribution as well as generalization performance. For the margin distribution of unlabeled data, as shown in the right panel, we observed a similar interesting phenomenon. ASSEMBLE and EntropyBoost have slightly greater margins when considering the bottom 20% unlabeled samples, but SSDBoost achieves a better margin distribution overall.

4 Conclusion

We have proposed a semi-supervised boosting method that directly optimizes classification errors and margins on both available labeled and unlabeled data. Coordinate descent/ascent based optimization algorithms are proposed to facilitate this idea. The results on both UCI datasets and a synthetic noisy dataset demonstrate the feasibility and advantages of this approach, and the observed robustness of SSDBoost suggests that it might be quite useful in practice.
Acknowledgments
This research is supported in part by AFOSR under grant FA9550-10-1-0335, NSF under grant IIS:RI-small 1218863, DoD under grant FA2386-13-1-3023, and a Google research award. We would like to thank the Ohio Supercomputer Center for an allocation of computing time to make this research possible.

References


