A Short Introduction to Boosting

Yoav Freund  Robert E. Schapire
AT&T Labs – Research
Shannon Laboratory
180 Park Avenue
Florham Park, NJ 07932 USA
www.research.att.com/~{yoav, schapire}
{yoav, schapire}@research.att.com

Abstract

Boosting is a general method for improving the accuracy of any given learning algorithm. This short overview paper introduces the boosting algorithm AdaBoost, and explains the underlying theory of boosting, including an explanation of why boosting often does not suffer from overfitting as well as boosting’s relationship to support-vector machines. Some examples of recent applications of boosting are also described.

Introduction

A horse-racing gambler, hoping to maximize his winnings, decides to create a computer program that will accurately predict the winner of a horse race based on the usual information (number of races recently won by each horse, betting odds for each horse, etc.). To create such a program, he asks a highly successful expert gambler to explain his betting strategy. Not surprisingly, the expert is unable to articulate a grand set of rules for selecting a horse. On the other hand, when presented with the data for a specific set of races, the expert has no trouble coming up with a “rule of thumb” for that set of races (such as, “Bet on the horse that has recently won the most races” or “Bet on the horse with the most favored odds”). Although such a rule of thumb, by itself, is obviously very rough and inaccurate, it is not unreasonable to expect it to provide predictions that are at least a little bit better than random guessing. Furthermore, by repeatedly asking the expert’s opinion on different collections of races, the gambler is able to extract many rules of thumb.

In order to use these rules of thumb to maximum advantage, there are two problems faced by the gambler: First, how should he choose the collections of races presented to the expert so as to extract rules of thumb from the expert that will be the most useful? Second, once he has collected many rules of thumb, how can they be combined into a single, highly accurate prediction rule?

Boosting refers to a general and provably effective method of producing a very accurate prediction rule by combining rough and moderately inaccurate rules of thumb in a manner similar to
that suggested above. This short paper overviews some of the recent work on boosting, focusing especially on the AdaBoost algorithm which has undergone intense theoretical study and empirical testing. After introducing AdaBoost, we describe some of the basic underlying theory of boosting, including an explanation of why it often tends not to overfit. We also describe some experiments and applications using boosting.

**Background**

Boosting has its roots in a theoretical framework for studying machine learning called the “PAC” learning model, due to Valiant [46]; see Kearns and Vazirani [32] for a good introduction to this model. Kearns and Valiant [30, 31] were the first to pose the question of whether a “weak” learning algorithm which performs just slightly better than random guessing in the PAC model can be “boosted” into an arbitrarily accurate “strong” learning algorithm. Schapire [38] came up with the first provable polynomial-time boosting algorithm in 1989. A year later, Freund [17] developed a much more efficient boosting algorithm which, although optimal in a certain sense, nevertheless suffered from certain practical drawbacks. The first experiments with these early boosting algorithms were carried out by Drucker, Schapire and Simard [16] on an OCR task.

**AdaBoost**

The AdaBoost algorithm, introduced in 1995 by Freund and Schapire [23], solved many of the practical difficulties of the earlier boosting algorithms, and is the focus of this paper. Pseudocode for AdaBoost is given in Fig. 1. The algorithm takes as input a training set \((x_1, y_1), \ldots, (x_m, y_m)\) where each \(x_i\) belongs to some *domain* or *instance space* \(X\), and each *label* \(y_i\) is in some label set \(Y\). For most of this paper, we assume \(Y = \{-1, +1\}\); later, we discuss extensions to the multiclass case. AdaBoost calls a given *weak* or *base learning algorithm* repeatedly in a series of rounds \(t = 1, \ldots, T\). One of the main ideas of the algorithm is to maintain a distribution or set of weights over the training set. The weight of this distribution on training example \(i\) on round \(t\) is denoted \(D_t(i)\). Initially, all weights are set equally, but on each round, the weights of incorrectly classified examples are increased so that the weak learner is forced to focus on the hard examples in the training set.

The weak learner’s job is to find a *weak hypothesis* \(h_t : X \rightarrow \{-1, +1\}\) appropriate for the distribution \(D_t\). The goodness of a weak hypothesis is measured by its *error*

\[
\epsilon_t = \Pr_{x \sim D_t} [h_t(x) \neq y] = \sum_{i : h_t(x_i) \neq y_i} D_t(i).
\]

Notice that the error is measured with respect to the distribution \(D_t\) on which the weak learner was trained. In practice, the weak learner may be an algorithm that can use the weights \(D_t\) on the training examples. Alternatively, when this is not possible, a subset of the training examples can be sampled according to \(D_t\), and these (unweighted) resampled examples can be used to train the weak learner.

Relating back to the horse-racing example, the instances \(x_i\) correspond to descriptions of horse races (such as which horses are running, what are the odds, the track records of each horse, etc.)
Given: $(x_1, y_1), \ldots, (x_m, y_m)$ where $x_i \in X, y_i \in Y = \{-1, +1\}$

Initialize $D_1(i) = 1/m$.

For $t = 1, \ldots, T$:

- Train weak learner using distribution $D_t$.
- Get weak hypothesis $h_t : X \to \{-1, +1\}$ with error
  \[ \epsilon_t = \Pr_{i \sim D_t} [h_t(x_i) \neq y_i]. \]

- Choose $\alpha_t = \frac{1}{2} \ln \left( \frac{1 - \epsilon_t}{\epsilon_t} \right)$.

- Update:
  \[
  D_{t+1}(i) = \frac{D_t(i)}{Z_t} \times \begin{cases} 
    e^{-\alpha_t} & \text{if } h_t(x_i) = y_i \\
    e^{\alpha_t} & \text{if } h_t(x_i) \neq y_i 
  \end{cases}
  \]
  \[= \frac{D_t(i) \exp(-\alpha_t y_i h_t(x_i))}{Z_t} \]

  where $Z_t$ is a normalization factor (chosen so that $D_{t+1}$ will be a distribution).

Output the final hypothesis:
\[
H(x) = \text{sign} \left( \sum_{t=1}^{T} \alpha_t h_t(x) \right).
\]

Figure 1: The boosting algorithm AdaBoost.

and the labels $y_i$ give the outcomes (i.e., the winners) of each race. The weak hypotheses are the rules of thumb provided by the expert gambler where the subcollections that he examines are chosen according to the distribution $D_t$.

Once the weak hypothesis $h_t$ has been received, AdaBoost chooses a parameter $\alpha_t$ as in the figure. Intuitively, $\alpha_t$ measures the importance that is assigned to $h_t$. Note that $\alpha_t \geq 0$ if $\epsilon_t \leq 1/2$ (which we can assume without loss of generality), and that $\alpha_t$ gets larger as $\epsilon_t$ gets smaller.

The distribution $D_t$ is next updated using the rule shown in the figure. The effect of this rule is to increase the weight of examples misclassified by $h_t$, and to decrease the weight of correctly classified examples. Thus, the weight tends to concentrate on “hard” examples.

The final hypothesis $H$ is a weighted majority vote of the $T$ weak hypotheses where $\alpha_t$ is the weight assigned to $h_t$.

Schapire and Singer [42] show how AdaBoost and its analysis can be extended to handle weak hypotheses which output real-valued or confidence-rated predictions. That is, for each instance $x$, the weak hypothesis $h_t$ outputs a prediction $h_t(x) \in \mathbb{R}$ whose sign is the predicted label ($-1$ or $+1$) and whose magnitude $|h_t(x)|$ gives a measure of “confidence” in the prediction. In this paper, however, we focus only on the case of binary ($\{-1, +1\}$) valued weak-hypothesis predictions.
Figure 2: Error curves and the margin distribution graph for boosting C4.5 on the letter dataset as reported by Schapire et al. [41]. Left: the training and test error curves (lower and upper curves, respectively) of the combined classifier as a function of the number of rounds of boosting. The horizontal lines indicate the test error rate of the base classifier as well as the test error of the final combined classifier. Right: The cumulative distribution of margins of the training examples after 5, 100 and 1000 iterations, indicated by short-dashed, long-dashed (mostly hidden) and solid curves, respectively.

Analyzing the training error

The most basic theoretical property of AdaBoost concerns its ability to reduce the training error. Let us write the error $\epsilon_t$ of $h_t$ as $\frac{1}{2} - \gamma_t$. Since a hypothesis that guesses each instance’s class at random has an error rate of $1/2$ (on binary problems), $\gamma_t$ thus measures how much better than random are $h_t$’s predictions. Freund and Schapire [23] prove that the training error (the fraction of mistakes on the training set) of the final hypothesis $H$ is at most

$$
\prod_t \left[ \frac{2\sqrt{\epsilon_t(1 - \epsilon_t)}}{\epsilon_t(1 - \epsilon_t)} \right] = \prod_t \sqrt{1 - 4\gamma_t^2} \leq \exp \left( -2 \sum_t \gamma_t^2 \right). \tag{1}
$$

Thus, if each weak hypothesis is slightly better than random so that $\gamma_t \geq \gamma$ for some $\gamma > 0$, then the training error drops exponentially fast.

A similar property is enjoyed by previous boosting algorithms. However, previous algorithms required that such a lower bound $\gamma$ be known a priori before boosting begins. In practice, knowledge of such a bound is very difficult to obtain. AdaBoost, on the other hand, is adaptive in that it adapts to the error rates of the individual weak hypotheses. This is the basis of its name — “Ada” is short for “adaptive.”

The bound given in Eq. (1), combined with the bounds on generalization error given below, prove that AdaBoost is indeed a boosting algorithm in the sense that it can efficiently convert a weak learning algorithm (which can always generate a hypothesis with a weak edge for any distribution) into a strong learning algorithm (which can generate a hypothesis with an arbitrarily low error rate, given sufficient data).
Generalization error

Freund and Schapire [23] showed how to bound the generalization error of the final hypothesis in terms of its training error, the sample size $m$, the VC-dimension $d$ of the weak hypothesis space and the number of boosting rounds $T$. (The VC-dimension is a standard measure of the “complexity” of a space of hypotheses. See, for instance, Blumer et al. [5].) Specifically, they used techniques from Baum and Haussler [4] to show that the generalization error, with high probability, is at most

$$\hat{\Pr} [H(x) \neq y] + O \left( \sqrt{\frac{T d}{m}} \right)$$

where $\hat{\Pr} [\cdot]$ denotes empirical probability on the training sample. This bound suggests that boosting will overfit if run for too many rounds, i.e., as $T$ becomes large. In fact, this sometimes does happen. However, in early experiments, several authors [9, 15, 36] observed empirically that boosting often does not overfit, even when run for thousands of rounds. Moreover, it was observed that AdaBoost would sometimes continue to drive down the generalization error long after the training error had reached zero, clearly contradicting the spirit of the bound above. For instance, the left side of Fig. 2 shows the training and test curves of running boosting on top of Quinlan’s C4.5 decision-tree learning algorithm [37] on the “letter” dataset.

In response to these empirical findings, Schapire et al. [41], following the work of Bartlett [2], gave an alternative analysis in terms of the margins of the training examples. The margin of
Figure 4: Comparison of error rates for AdaBoost and four other text categorization methods (naive Bayes, probabilistic TF-IDF, Rocchio and sleeping experts) as reported by Schapire and Singer [43]. The algorithms were tested on two text corpora — Reuters newswire articles (left) and AP newswire headlines (right) — and with varying numbers of class labels as indicated on the x-axis of each figure.

example \((x, y)\) is defined to be

\[
y \sum_{t} \alpha_t h_t(x) \frac{1}{\sum_{t} \alpha_t}.
\]

(2)

It is a number in \([-1, +1]\) which is positive if and only if \(H\) correctly classifies the example. Moreover, the magnitude of the margin can be interpreted as a measure of confidence in the prediction. Schapire et al. proved that larger margins on the training set translate into a superior upper bound on the generalization error. Specifically, the generalization error is at most

\[
\hat{\Pr} \left[ \text{margin} (x, y) \leq \theta \right] + O \left( \sqrt{\frac{d}{mT^2}} \right)
\]

(3)

for any \(\theta > 0\) with high probability. Note that this bound is entirely independent of \(T\), the number of rounds of boosting. In addition, Schapire et al. proved that boosting is particularly aggressive at reducing the margin (in a quantifiable sense) since it concentrates on the examples with the smallest margins (whether positive or negative). Boosting’s effect on the margins can be seen empirically, for instance, on the right side of Fig. 2 which shows the cumulative distribution of margins of the training examples on the “letter” dataset. In this case, even after the training error reaches zero, boosting continues to increase the margins of the training examples effecting a corresponding drop in the test error.

Attempts (not always successful) to use the insights gleaned from the theory of margins have been made by several authors [7, 27, 34].

The behavior of AdaBoost can also be understood in a game-theoretic setting as explored by Freund and Schapire [22, 24] (see also Grove and Schuurmans [27] and Breiman [8]). In particular, boosting can be viewed as repeated play of a certain game, and AdaBoost can be shown to be a
special case of a more general algorithm for playing repeated games and for approximately solving a game. This also shows that boosting is closely related to linear programming and online learning.

Relation to support-vector machines

The margin theory points to a strong connection between boosting and the support-vector machines of Vapnik and others [6, 12, 47]. To clarify the connection, suppose that we have already found the weak hypotheses that we want to combine and are only interested in choosing the coefficients $\alpha_t$. One reasonable approach suggested by the analysis of AdaBoost’s generalization error is to choose the coefficients so that the bound given in Eq. (3) is minimized. In particular, suppose that the first term is zero and let us concentrate on the second term so that we are effectively attempting to maximize the minimum margin of any training example. To make this idea precise, let us denote the vector of weak-hypothesis predictions associated with the example $(x, y)$ by $h(x) = \langle h_1(x), h_2(x), \ldots, h_N(x) \rangle$ which we call the instance vector and the vector of coefficients by $\alpha = \langle \alpha_1, \alpha_2, \ldots, \alpha_N \rangle$ which we call the weight vector. Using this notation and the definition of margin given in Eq. (2) we can write the goal of maximizing the minimum margin as

$$\max_{\alpha} \min_i \frac{(\alpha \cdot h(x_i)) y_i}{||\alpha|| \cdot ||h(x_i)||}$$

(4)

where, for boosting, the norms in the denominator are defined as:

$$||\alpha||_1 = \sum_t |\alpha_t|, \quad ||h(x)||_\infty = \max_t |h_t(x)|.$$  

(When the $h_t$’s all have range $\{-1, +1\}$, $||h(x)||_\infty$ is simply equal to 1.)

In comparison, the explicit goal of support-vector machines is to maximize a minimal margin of the form described in Eq. (4), but where the norms are instead Euclidean:

$$||\alpha||_2 = \sqrt{\sum_t \alpha_t^2}, \quad ||h(x)||_2 = \sqrt{\sum_t h_t(x)^2}.$$  

Thus, SVM’s use the $\ell_2$ norm for both the instance vector and the weight vector, while AdaBoost uses the $\ell_\infty$ norm for the instance vector and $\ell_1$ norm for the weight vector.

When described in this manner, SVM and AdaBoost seem very similar. However, there are several important differences:

- **Different norms can result in very different margins.** The difference between the norms $\ell_1$, $\ell_2$ and $\ell_\infty$ may not be very significant when one considers low dimensional spaces. However, in boosting or in SVM, the dimension is usually very high, often in the millions or more. In such a case, the difference between the norms can result in very large differences

1Of course, AdaBoost does not explicitly attempt to maximize the minimal margin. Nevertheless, Schapire et al.’s [41] analysis suggests that the algorithm does try to make the margins of all the training examples as large as possible, so in this sense, we can regard this maximum minimal margin algorithm as an illustrative approximation of AdaBoost. In fact, algorithms that explicitly attempt to maximize minimal margin have not been experimentally as successful as AdaBoost [7, 27].
in the margin values. This seems to be especially so when there are only a few relevant variables so that \(\alpha\) can be very sparse. For instance, suppose the weak hypotheses all have range \([-1, +1]\) and that the label \(y\) on all examples can be computed by a majority vote of \(k\) of the weak hypotheses. In this case, it can be shown that if the number of relevant weak hypotheses \(k\) is a small fraction of the total number of weak hypotheses then the margin associated with AdaBoost will be much larger than the one associated with support vector machines.

- **The computation requirements are different.** The computation involved in maximizing the margin is mathematical programming, i.e., maximizing a mathematical expression given a set of inequalities. The difference between the two methods in this regard is that SVM corresponds to quadratic programming, while AdaBoost corresponds only to linear programming. (In fact, as noted above, there is a deep relationship between AdaBoost and linear programming which also connects AdaBoost with game theory and online learning [22].)

- **A different approach is used to search efficiently in high dimensional space.** Quadratic programming is more computationally demanding than linear programming. However, there is a much more important computational difference between SVM and boosting algorithms. Part of the reason for the effectiveness of SVM and AdaBoost is that they find linear classifiers for extremely high dimensional spaces, sometimes spaces of infinite dimension. While the problem of overfitting is addressed by maximizing the margin, the computational problem associated with operating in high dimensional spaces remains. Support vector machines deal with this problem through the method of kernels which allow algorithms to perform low dimensional calculations that are mathematically equivalent to inner products in a high dimensional “virtual” space. The boosting approach is instead to employ greedy search: from this perspective, the weak learner is an oracle for finding coordinates of \(h(x)\) that have a non-negligible correlation with the label \(y\). The reweighting of the examples changes the distribution with respect to which the correlation is measured, thus guiding the weak learner to find different correlated coordinates. Most of the actual work involved in applying SVM or AdaBoost to specific classification problems has to do with selecting the appropriate kernel function in the one case and weak learning algorithm in the other. As kernels and weak learning algorithms are very different, the resulting learning algorithms usually operate in very different spaces and the classifiers that they generate are extremely different.

**Multiclass classification**

So far, we have only considered binary classification problems in which the goal is to distinguish between only two possible classes. Many (perhaps most) real-world learning problems, however, are multiclass with more than two possible classes. There are several methods of extending AdaBoost to the multiclass case.

The most straightforward generalization [23], called AdaBoost.M1, is adequate when the weak learner is strong enough to achieve reasonably high accuracy, even on the hard distributions created by AdaBoost. However, this method fails if the weak learner cannot achieve at least 50% accuracy when run on these hard distributions.
Figure 5: A sample of the examples that have the largest weight on an OCR task as reported by Freund and Schapire [21]. These examples were chosen after 4 rounds of boosting (top line), 12 rounds (middle) and 25 rounds (bottom). Underneath each image is a line of the form $d: \ell_1/w_1, \ell_2/w_2$, where $d$ is the label of the example, $\ell_1$ and $\ell_2$ are the labels that get the highest and second highest vote from the combined hypothesis at that point in the run of the algorithm, and $w_1, w_2$ are the corresponding normalized scores.

For the latter case, several more sophisticated methods have been developed. These generally work by reducing the multiclass problem to a larger binary problem. Schapire and Singer’s [42] algorithm AdaBoost.MH works by creating a set of binary problems, for each example $x$ and each possible label $y$, of the form: “For example $x$, is the correct label $y$ or is it one of the other labels?” Freund and Schapire’s [23] algorithm AdaBoost.M2 (which is a special case of Schapire and Singer’s [42] AdaBoost.MR algorithm) instead creates binary problems, for each example $x$ with correct label $y$ and each incorrect label $y'$ of the form: “For example $x$, is the correct label $y$ or $y'$?”

These methods require additional effort in the design of the weak learning algorithm. A different technique [39], which incorporates Dietterich and Bakiri’s [14] method of error-correcting output codes, achieves similar provable bounds to those of AdaBoost.MH and AdaBoost.M2, but can be used with any weak learner which can handle simple, binary labeled data. Schapire and Singer [42] give yet another method of combining boosting with error-correcting output codes.
Experiments and applications

Practically, AdaBoost has many advantages. It is fast, simple and easy to program. It has no parameters to tune (except for the number of round $T$). It requires no prior knowledge about the weak learner and so can be flexibly combined with any method for finding weak hypotheses. Finally, it comes with a set of theoretical guarantees given sufficient data and a weak learner that can reliably provide only moderately accurate weak hypotheses. This is a shift in mind set for the learning-system designer: instead of trying to design a learning algorithm that is accurate over the entire space, we can instead focus on finding weak learning algorithms that only need to be better than random.

On the other hand, some caveats are certainly in order. The actual performance of boosting on a particular problem is clearly dependent on the data and the weak learner. Consistent with theory, boosting can fail to perform well given insufficient data, overly complex weak hypotheses or weak hypotheses which are too weak. Boosting seems to be especially susceptible to noise [13] (more on this later).

AdaBoost has been tested empirically by many researchers, including [3, 13, 15, 29, 33, 36, 45]. For instance, Freund and Schapire [21] tested AdaBoost on a set of UCI benchmark datasets [35] using C4.5 [37] as a weak learning algorithm, as well as an algorithm which finds the best “decision stump” or single-test decision tree. Some of the results of these experiments are shown in Fig. 3. As can be seen from this figure, even boosting the weak decision stumps can usually give as good results as C4.5, while boosting C4.5 generally gives the decision-tree algorithm a significant improvement in performance.

In another set of experiments, Schapire and Singer [43] used boosting for text categorization tasks. For this work, weak hypotheses were used which test on the presence or absence of a word or phrase. Some results of these experiments comparing AdaBoost to four other methods are shown in Fig. 4. In nearly all of these experiments and for all of the performance measures tested, boosting performed as well or significantly better than the other methods tested. Boosting has also been applied to text filtering [44], “ranking” problems [19] and classification problems arising in natural language processing [1, 28].

The generalization of AdaBoost by Schapire and Singer [42] provides an interpretation of boosting as a gradient-descent method. A potential function is used in their algorithm to associate a cost with each example based on its current margin. Using this potential function, the operation of AdaBoost can be interpreted as a coordinate-wise gradient descent in the space of linear classifiers (over weak hypotheses). Based on this insight, one can design algorithms for learning popular classification rules. In recent work, Cohen and Singer [11] showed how to apply boosting to learn rule lists similar to those generated by systems like RIPPER [10], IREP [26] and C4.5 rules [37]. In other work, Freund and Mason [20] showed how to apply boosting to learn a generalization of decision trees called “alternating trees.”

A nice property of AdaBoost is its ability to identify outliers, i.e., examples that are either mislabeled in the training data, or which are inherently ambiguous and hard to categorize. Because AdaBoost focuses its weight on the hardest examples, the examples with the highest weight often turn out to be outliers. An example of this phenomenon can be seen in Fig. 5 taken from an OCR experiment conducted by Freund and Schapire [21].

When the number of outliers is very large, the emphasis placed on the hard examples can
become detrimental to the performance of AdaBoost. This was demonstrated very convincingly by Dietterich [13]. Friedman et al. [25] suggested a variant of AdaBoost, called “Gentle AdaBoost” which puts less emphasis on outliers. In recent work, Freund [18] suggested another algorithm, called “BrownBoost,” which takes a more radical approach that de-emphasizes outliers when it seems clear that they are “too hard” to classify correctly. This algorithm is an adaptive version of Freund’s [17] “boost-by-majority” algorithm. This work, together with Schapire’s [40] work on “drifting games,” reveal some interesting new relationships between boosting, Brownian motion, and repeated games while raising many new open problems and directions for future research.

References


