Robust Multi-Class Boosting

Gunnar Rätsch

Fraunhofer FIRST
Kekuléstr. 7, 12489 Berlin, Germany
Gunnar.Raetsch@first.fhg.de

Max-Planck Institute for Biol. Cybernetics
Spemannstr. 38, 72076 Tübingen, Germany
Gunnar.Raetsch@tuebingen.mpg.de

Abstract

Boosting approaches are based on the idea that high-quality learning algorithms can be formed by repeated use of a “weak-learner”, which is required to perform only slightly better than random guessing. It is known that Boosting can lead to drastic improvements compared to the individual weak-learner. For two-class problems it has been shown that the original Boosting algorithm, called AdaBoost, is quite unaffected by overfitting. However, for the case of noisy data, it is also understood that AdaBoost can be improved considerably by introducing some regularization technique.

In speech-related problems one often considers multi-class problems and Boosting formulations have been used successfully to solve them. I review existing multi-class boosting algorithms, which have been much less analyzed and explored than the two-class problems. In this work I extend these methods to derive new boosting algorithms which are more robust against outliers and noise in the data and are able to exploit prior knowledge about relationships between the classes.

1. Introduction

Boosting is a technique for sequentially training and combining a collection of classifiers in such a way that the later classifiers adjust for the deficiencies of the earlier ones. Many variants exists and a few of them I will briefly review in this work. They all follow the same basic strategy: There is a sequence of iterations, and at each iteration a new classifier is trained on a weighted training set. Initially, every example gets the same weight, but in later iterations, the weights of hard-to-classify examples are increased relative to the easy ones.

Experimental results in a variety of classifications tasks have shown AdaBoost’s remarkable success in improving the classifier accuracy (cf. [1] and references therein). This is supported by the theoretical analysis in [2] showing that AdaBoost is effective in increasing the separation margin between the classes, which plays a crucial role in bounding the generalization error of the resulting combined classifier. Large margin algorithms as Support Vector Machines and Boosting are nowadays the state-of-the-art in machine learning [3].

In speech recognition, however, there are only a few studies applying boosting to acoustic models: in continuous speech recognition [4], in voice-mail transcription [5] and utterance classification [6, 7]. This small number of applications in speech recognition is surprising as it seems particularly simple to use boosting techniques with frequently used Hidden Markov models and, hence, to combine the benefits of a well-tuned probabilistic model for speech recognition with the state-of-the-art large margin concept from machine learning.

In some of the mentioned applications remarkable improvements using boosting were observed. In other cases, however, only minor or no improvements could be achieved. I suspect that this is mainly due to used multi-class boosting formulation (AdaBoost.M2). As in the binary case, this formulation implicitly assumes that the data is separable and may overemphasize examples that are hard to classify. For the binary case, robust versions of AdaBoost have been developed: They “give up” on hard-to-learn examples, which led to great improvements in many experiments (cf. [1] and references therein). Those methods still generate large margins, but incorporate the idea of a soft-margin which also made the practical success of Support-Vector-Machines [8] possible.

In this work I propose an improvement of current boosting algorithms for the multi-class case by incorporating the soft-margin concept. I start with a brief review in Section 2 of existing boosting methods. In Section 3, I generalize the margin definition, then outline the robustified algorithm and discuss several extensions and modifications which seem appropriate for use in a speech recognition system. Finally I give a few details of the derivation of the algorithm and conclude with a brief discussion in Section 4.

2. Multi-Class Boosting

The purpose of boosting is to find a highly accurate classification rule by combining many weak or base hypotheses, each of which may only be moderately accurate. It is assumed to have access to a separate procedure called the weak learner or weak learning algorithm for computing the weak hypotheses. The boosting algorithm calls the weak learner repeatedly in a series of rounds and so finds a set of weak hypotheses. Those are then linearly combined into a single rule – the final or combined hypothesis.

In the simplest version of AdaBoost for multi-class classification, called AdaBoost.M1 [9], the algorithm maintains a set of importance weights over the training examples. These weights are used by the weak learning algorithm whose goal is to find a weak hypothesis with moderately low weighted error. AdaBoost.M1 uses the weights to force the weak learning algorithm to concentrate on the examples which are hardest to classify [10].

Later it was found that it is more appropriate to maintain a distribution on the examples and the labels. As boosting progresses training examples and their corresponding labels that are hard to predict correctly, get incrementally higher weights than the other examples and labels. The intended effect is to force the weak learner to concentrate on examples and labels that will be most beneficial to the overall goal of finding a highly accurate classification rule [10].

2.1. AdaBoost.M2

The latter idea is implemented in AdaBoost.M2 (cf. Algorithm 1) as proposed in [9]. One starts with the uniform distribution on the examples and then calls the weak learner, which returns a hypothesis \( h_t : x \rightarrow [0, 1]^C \), where \( C \) is the number of classes, i.e., for every example it assigns a score in the range \([0, 1]\) for each class \( c = 1, \ldots, C \). I denote by \( h^c(x) \) the \( c \)-th component of \( h(x) \). The quality of the new hypothesis is given by the pseudo-loss \( \epsilon_t \in [0, 1] \), which is equal to a half minus the weighted average difference of the correct class-score and any
Algorithm 1 The AdaBoost.M2 algorithm

1. Input: \( N \) examples \( Z = \{(x_1, y_1), \ldots, (x_N, y_N)\} \), Number of iterations \( T \)

2. Initialize: \( d_{0,c}^{(1)} = 1/(C-1) \)

3. Do for \( t = 1, \ldots, T \):
   
   (a) Train classifier with respect to the weighted examples and obtain hypothesis \( h_t : x \mapsto [0, 1]^C \) with small pseudo-loss
   
   \[ \epsilon_t = \frac{1}{\sum_{n,c \neq y_n} d_{n,c}^{(t)} (1 - h^n_t(x_n) + h^n_t(x_n))} \]

   (b) Let \( \alpha_t = \frac{1}{2} \log \frac{1 - \epsilon_t}{\epsilon_t} \)

   (c) Update
   
   \[ d_{n,c}^{(t+1)} = \frac{d_{n,c}^{(t)}}{Z_t} \exp (-\alpha_t (1 + y_n h^n_t(x_n) - h^n_t(x_n))) \]

   where \( Z_t \) is such that \( \sum_{n,c \neq y_n} d_{n,c}^{(t+1)} = 1 \).

4. Output: Final hypothesis with weights \( \alpha^{(T)} \):

\[ f(x) = \sum_{t=1}^{T} \sum_{c} \alpha_t h_t(x) \]

other class-score (cf. step 3a in Algorithm 1). Hence, if in most cases \( h^n_t(x_n) - h^n_t(x_n - h^n_t(x_n)) \) holds, then \( \epsilon_t \) will be considerably smaller than \( \frac{1}{2} \). It can be shown that if the base learner always returns a hypothesis with pseudo-loss consistently smaller than \( \frac{1}{2} \), then the training error of the combined hypothesis will converge fast to zero. For the final hypothesis \( f : x \mapsto \mathbb{R}^C \) holds in this case:

\[ f^n(x_n) - \max_{c \neq y_n} f^c(x_n) > 0, \]

for all \( n = 1, \ldots, N \), i.e. the data is separated. In the following I will call the left-hand-side of (1) the margin of the example \( x_n \).

In binary classification, the margin corresponds to the separation distance between the linearly separated classes. From a theoretical point of view it is beneficial, as for large-margin two-class classification, to maximize the separation between the classes if the data is noise-free and separable. AdaBoost.M2 tries to achieve this, but as for binary AdaBoost it could not be shown that it maximizes the separation distance. However, if the data is noisy – as often in speech recognition – then the pure large margin strategy turns out to be sub-optimal. In this case AdaBoost overemphasizes some examples in order to classify them right – the algorithm becomes very sensible to such examples and tends to overfit. Here, the soft-margin idea (as proposed for binary classification in [12]) will help making the algorithm more robust against noise.

2.2. Logistic Regression

A different algorithm was proposed in [13]. For simplicity let us use the following notation: let \( y_n \), be the \( C \)-dimensional vector of the form \( (0, 0, \ldots, 0, 1, 0, \ldots, 0) \) with a 1 in the \( c \)-th position if, and only if, \( x_n \) belongs to the \( c \)-th class. In [13] the log-likelihood function:

\[ G = \sum_{n=1}^{N} \sum_{c=1}^{C} \{ y_{n,c} \log p(c|x_n) + (1 - y_{n,c}) \log (1 - p(c|x_n)) \} \]

was considered, where \( y_{n,c} \) is the \( c \)-th component of the vector \( y_n \), and \( p(c|x_n) \) is the model probability that \( x_n \) belongs to the \( c \)-th class. The standard soft-max representation, \( p(c|x) = \frac{\exp(f^c(x))}{\sum_{c'=1}^{C} \exp(f^{c'}(x))} \), where \( f^c(x) \) is the \( c \)-th component of the combined hypothesis, was used to obtain a probability vector from the combined hypothesis \( f(x) \). Then using an algorithm similar to Algorithm 1, but using a different weighting scheme and some additional optimization methods, one can iteratively find a combined hypothesis that maximizes the log-likelihood. The clear probabilistic modeling seems nice, but the important concept of the large margin classification is missing in this approach. However, since examples are not overemphasized too much, Logistic Regression worked in noisy cases considerably better than AdaBoost.M2 [13]. But since an appropriate way of complexity control is missing, I expect it to overfit easily as one continues to combine weak hypotheses. The proposed algorithm in Section 3 uses similar weight updates and also exhibits the mentioned robustness against noise, while having the large margin concept incorporated.

2.3. Error Correcting Codes

There has recently been extensive activity on recoding multi-class problems as a sequence of binary problems, using the idea of error-correcting codes [14]. A detailed description of the approach can be found in [15] in a general context as well as in the Boosting setup. Two special cases of this general approach are the so-called one-against-all and all-pairs approaches, which were extensively used prior to the development of the error correcting code approach. In the former case, given a \( C \)-class classification problem, one constructs \( C \) binary classifiers each of which learns to distinguish one class from the rest. The multi-category classification then uses the highest ranking classifier. In the all-pairs approach, all possible \( \binom{C}{2} \) pairs of classification problems are learned and used to form the multi-category classifier using some form of majority voting. Although these techniques seem very promising, to my knowledge those techniques have not yet been applied to speech recognition (at least the all-pairs approach seems infeasible when having many classes). In the next section I will discuss an approach which is based on real-valued codes but their use is differently motivated than in e.g. [14].

3. A Robust Multi-Class Algorithm

3.1. Margins and Codes

Before I present the new algorithm, I generalize the definition of the margin as used before in (1). Let us consider the problem of \( C \) classes and \( N \) training examples \( (x_n, y_n) \) \( \in \mathcal{X} \times \{1, \ldots, C\} \). Suppose one is given a set of code vectors \( t_c, c = 1, \ldots, C \). For simplicity assume \( t_c \in \mathbb{R}^C \equiv \mathcal{C} \) and \( \|t_c\| = 1 \). Then one can reformulate the classification problem as follows: Try to find a function \( f : \mathcal{X} \rightarrow \mathcal{C} \) that maps examples of the \( c \)-th class close to its code vector \( t_c \) and far from all the other vectors. Then it is natural to define the margin \( \rho \) of \( f \) at example \( (x_n, y_n) \) as follows:

\[ \rho(f(x), y) := \min_{c \neq y_n} d(t_c, f(x)) - d(t_{y_n}, f(x)), \]

where \( d \) is some distance measure between code and mapped example. It has been shown in [16] that in order to obtain a convex optimization problem (and thus ensure efficiency in optimization), the distance has to have the following form \( d(a, b) = d_1(a) + d_2(b) + \lambda^\top B b \), where \( d_1 \) and \( d_2 \) are convex functions and the matrix \( B \) is symmetric. The simplest case is the squared Euclidean distance, which I will assume here, but other distance measures might be more appropriate. For the Euclidean distance, (2) simplifies to

\[ \rho(f(x), y) := \min_{c \neq y_n} (t_c - t_{y_n})^\top f(x), \]

where I used the assumption \( \|t_c\| = \|t_{y_n}\| = 1 \).

Let us consider the case, where the code vectors are simply the unit vectors, i.e. \( t_c = e_c \). Then (3) simplifies to the original
margin definition in (1). The following derivations and the algorithm are formulated using this more general notion of margin, but it can easily be translated back to the original setting.

But why is it useful to have these code vectors? I can only give an intuition. Suppose one has many different classes (as in speech recognition), then some of these classes will be very similar (e.g. ‘here’ and ‘beer’), while others have nothing in common (‘sausage’ and ‘bread’). Moreover, assume one knows these relationships a priori and has a set of code vectors available that reflect these class relations. Then it would be relatively easy to learn a function that maps examples of similar classes into the right area of the code space – even with a very coarse model. What is left is to learn the fine level class separation which I believe is easier if the code vectors appropriately reflect the class relationships.

In [16] we proposed an algorithm that automatically learns such relationships, but the large number of classes in speech recognition would make a direct application of this approach infeasible. However, existing prior knowledge could be used to find a good set of code vectors and if this knowledge is not available, then the default unit code vectors have to suffice.

Algorithm 2 The AdaBoost.M2 algorithm

1. **Input:** \( N \) examples \( Z = \{ (x_1, y_1), \ldots, (x_N, y_N) \} \). Number of iterations \( T \), Regularization constant \( \nu \) (e.g. \( \nu = 0.2 \)), approximation constant \( \beta > 0 \) (e.g. \( \beta = 1/100 \)), a set of \( C \) code vectors \( t_c \in \mathbb{R}^C \) (e.g. \( t_c = e_c \)).

2. **Initialize:** \( d^{(1)}_{n,c} = 1, \alpha^{(0)} = e^{(1)} = 1^{\text{st}} \) unit vector.

3. **Do for** \( t = 1, \ldots, T \):
   a) Train classifier with respect to the weighted examples and obtain hypothesis \( h_t : x \mapsto \mathbb{R}^C \) with small pseudo-loss as in (5).
   b) Find best trade-off between new and old hypotheses by minimizing \( E(\varrho, \alpha) \) as defined in (4)\footnote{For AdaBoost.M2 there is also such cost function [17], which can be minimized instead of using the explicit solution.}
   \[
   \left[ \varrho^{(t)}, \alpha^{(t)} \right] = \operatorname{argmin}_{\varrho, \alpha} E(\varrho, \alpha) \quad \alpha^{(t)} = (1 - \lambda)\alpha^{(t-1)}
   \]
   c) Let \( \alpha^{(t)} = \frac{\lambda}{(1 - \lambda)} \alpha^{(t-1)} + (1 - \lambda) \alpha^{(t-1)} \)
   d) Let \( \rho_{n,c} = (y_n - c)^T f_{\alpha^{(t)}}(x_n) \)
   e) Update \( d^{(t)}_{n,c} = \frac{\exp \left( \frac{\varrho_n - \rho_{n,c}}{\beta} \right)}{1 + \exp \left( \frac{\varrho_n - \rho_{n,c}}{\beta} \right)} \)

4. **Output:** Final hypothesis with weights \( \alpha^{(T)} \):
   \[
   f_{\alpha^{(T)}}(x) = \sum_{t=1}^{T} \alpha^{(t)} h_t(x)
   \]

3.2. The Algorithm

The proposed algorithm is outlined in Algorithm 2. It works along the same lines as AdaBoost.M2. The main differences are a) the computation of the hypothesis coefficient \( \alpha_t \) and b) a different weighting scheme for the examples. Moreover, it has two additional parameters \( \nu \) and \( \beta \), which I will discuss below.

a) In AdaBoost.M2, one computes the hypothesis coefficient \( \alpha_t \) at iteration \( t \) and normalizes the vector at the end. This is equivalent to keeping the length of \( \alpha_t \) equal to 1 and by letting the new weight vector \( \alpha^{(t)} \) be a convex combination of the old weight vector \( \alpha^{(t-1)} \) and the \( t \)-th unit vector \( e_t \) as in step 3c. The weighting is determined by \( \lambda_t \), which is determined in step 3b by minimizing the following loss function:

\[
E(\varrho, \alpha) = \beta \sum_{n,c \neq y_n} \left[ 1 + e^{-\varrho_n - \rho_{n,c}} \beta \right] - N(C - 1)\varrho \quad \text{(4)}
\]

where \( \rho_{n,c} \) is as in step 3d. In AdaBoost.M2 there is an explicit formula to compute \( \alpha_t \), which only approximates the optimal value when \( h \) is real valued [17]. Since this is often the case in speech recognition and every call to the weak learner can be very costly, it seems mandatory to accurately determine the optimal \( \alpha_t \) in each iteration to speed up the convergence.\footnote{For AdaBoost.M2 there is also such cost function [17], which can be minimized instead of using the explicit solution.}

b) The weighting in step 3e works different as in AdaBoost.M2. For simplicity, I use the explicit form instead of the iteratively updated distribution. Now one can readily see the effect on the weights: if the margin \( \rho_{n,c} \) is much larger than \( \varrho \), then the weight will be close to zero, but if it is much smaller, then it will be close to 1. In the extreme case of \( \varrho \to 0 \) holds: \( d^{(t)}_{n,c} = 1 \), if \( \rho_{n,c} < \varrho \) and \( d^{(t)}_{n,c} = 0 \), if \( \rho_{n,c} > \varrho \). Here one can see that the variable \( \varrho \) directly controls how many of the weights are non-zero. I will discuss in the next section that if one minimizes the function \( E \) with respect to \( \varrho \) (when \( \beta \to 0 \), then it is chosen such that the fraction of \( d \)’s which are non-zero is (almost) equal to \( \nu \) (the hyper-parameter). Thus, \( \nu \in [0, 1] \) allows one to control easily the fraction of margin errors and provides an interpretable way to control the complexity of the ensemble. The interpretability makes model selection often much easier (\( \nu = 0.2 \) works very well in many cases).

The parameter \( \beta \) controls how well this so-called \( \nu \)-property is satisfied. For too large \( \beta \) the approximation will only be fair. As one decreases \( \beta \), then the approximation quality improves, but the function \( E \) becomes less and less smooth, the optimization harder and the convergence to the optimum slower.

Finally, note that the algorithm only progresses if the base learner is able to return a weak hypothesis with small pseudo-loss. In the most general case, the pseudo-loss uses the code vectors

\[
\gamma_t = \sum_{n,c \neq y_n} d^{(t)}_{n,c} (y_n - c^T h_t(x_n))
\]

If one uses the trivial code, this definition is up to constants equal to the one used in step 3a in Algorithm 1. One can show, that if \( \gamma_t > 0 \) then the optimal \( \lambda_t \) is equal zero and the algorithm stops making progress.

3.3. Remarks

Let me briefly discuss two questions: a) How should one use the weights \( d_{n,c} \) in the base learner? b) How can one reduce the large number of weights when training with many classes?

a) In [9] it was proposed to provide the weak learner only with a “marginal weighting” on the examples \( D_n = \frac{1}{N} \sum_{c \neq y_n} d_{n,c} \), where \( Z \) is such that \( \sum_n D_n = 1 \). This strategy seems particularly useful, when the classes are trained separately using ML only using (positive) the examples of the corresponding class. However, this ignores the case when an example is well separated to one class \( c_1 \neq y_n \) but not from another class \( c_2 \neq y_n \). In order to take this into account, discriminative training seems more appropriate which makes it possible to force the learning algorithm to discriminate better between \( c_1 \) and \( y_n \) for this example. A first step in this direction was done in [6], which led to considerable improvements.

b) As noted before by [5, 6, 18], the computation of the weights \( d_{n,c} \) makes it necessary to compute the output of \( h \) for each example for every class which can be computationally too expensive. The proposed method is to use a \( M \)-best list \( L_m \) for each example \( x_n \), and then separate only against the classes in this list. This reduces the number of weights from \( (C - 1)N \) to \( MN (M < C) \). As discussed before, the fraction of non-zero weights \( d_{n,c} \) is determined by \( \nu \). In order to take the proposed restriction into account one either has to change the constant in (4) from \( N(C - 1) \)
to $NM$ leading to the appropriate meaning of the parameter $\nu$, or one has to make sure that $M > \nu(C-1)$ such that the algorithm is able to satisfy the $\nu$-property.

3.4. Sketch of the Derivation of the Algorithm

I started with the following optimization problem, which similarly appeared in [16]:

$$\min_{\alpha \in \mathcal{S}_T} \sum_{n=1}^{N} \sum_{c \neq y_n} \xi_{n,c} - \nu N(C-1) \theta$$

(6)

where $$(t_{n,y_n} - t_{n})^T f_{\alpha}(x_n) \geq \theta - \xi_{n,c},$$

one would like to find a convex combination $f_{\alpha}(x) = \sum_{c} \alpha_c h_c(x)$ of base hypotheses $h_1, h_2, \ldots$ that has as large as possible margin $(t_{n,y_n} - t_{n})^T f_{\alpha}(x_n)$. I use slack variables $\xi_{n,c}$ to allow for smaller margins than $\theta$ and misclassifications. In (6) one minimizes the sum of all slack variables (the margin errors) and at the same time maximizes the margin $\theta$.

The solution of (6) has the following property (cf. [19, 11]):

Suppose the solution of (6) satisfies $\theta > 0$, then

1. $\nu$ upper-bounds the fraction of margin errors ($\xi_{n,c} > 0$).
2. $1 - \nu$ is an upper bound on the fraction of examples with a margin $\min_{x \neq y_n}(t_{n,y_n} - t_{n})^T f_{\alpha}(x_n)$ larger than $\theta$.

Hence, the parameter $\nu$ can be interpreted as the fraction of examples (and labels) in the training set, where the separation to one of the other classes is smaller than $\theta$. For noisy data one would set this parameter larger and for well separable data close to zero (e.g. $\nu < 1/N(C-1)$).

It can easily be verified that the solution of (6) satisfies

$$\xi_{n,c} = \max(0, \theta - (t_{n,y_n} - t_{n})^T f_{\alpha}(x_n)).$$

This expression can be plugged into (6) and one obtains a non-smooth function in $\theta$ and $\alpha$. It is beneficial from an optimization point of view to replace $\max(0, \theta - \alpha)$ with $\beta \log \left[1 + \exp \left(\frac{\theta}{\beta} - \alpha\right)\right]$, where $\beta$ is a parameter which controls the smoothness and the quality of the approximation. It is easily verified that the approximation is exact for $\beta \to 0$. Finally I have the following objective to minimize

$$\beta \sum_{n,c \neq y_n} \left[1 + \exp \left(\frac{\theta - (t_{n,y_n} - t_{n})^T f_{\alpha}(x_n)}{\beta}\right)\right] - \nu N(C-1) \theta,$$

subject to $\alpha \in \mathcal{S}_T$ and $\theta > 0$. This objective is to be minimized over the set of all convex combinations of functions which can be generated by the base learner. I conjecture that by using the results in [20], one can show the convergence of Algorithm 2 to the minimum of (4), which approximately solves (6). Note that one could extend Algorithm 2 to appropriately decrease $\beta$ to zero (as e.g. in [11]). Using the standard theory of barrier optimization one can then show the convergence to the solution of the linear program (6) (cf. [11, 21] for more details).

4. Conclusion

In this work I proposed a new boosting algorithm for multi-class problems. It works similar as the original AdaBoost.M2 algorithm, but incorporates the soft-margin concept which improved the classification performance in many cases in binary problems. It combines the robustness against noise and outliers in the data as previously seen in Logistic Regression with large margins. Moreover, I discussed how to take prior knowledge about class relationships into account, which seems very important when learning about problems with many classes. It is future work to test and apply the proposed technique in a speech recognizer.

References