Robust Boosting for Regression Problems

Xiaomeng Ju*, Matías Salibián-Barrera
Department of Statistics
University of British Columbia

Abstract
The gradient boosting algorithm constructs a regression estimator using a linear combination of simple “base learners”. In order to obtain a robust non-parametric regression estimator that is scalable to high dimensional problems we propose a robust boosting algorithm based on a two-stage approach, similar to what is done for robust linear regression: we first minimize a robust residual scale estimator, and then improve its efficiency by optimizing a bounded loss function. Unlike previous proposals, our algorithm does not need to compute an ad-hoc residual scale estimator in each step. Since our loss functions are typically non-convex, we propose initializing our algorithm with an \(L_1\) regression tree, which is fast to compute. We also introduce a robust variable importance metric for variable selection that is calculated via a permutation procedure. Through simulated and real data experiments, we compare our method against gradient boosting with squared loss and other robust boosting methods in the literature. With clean data, our method works equally well as gradient boosting with the squared loss. With symmetric and asymmetrically contaminated data, we show that our proposed method outperforms in terms of prediction error and variable selection accuracy.

Keywords: Regression, Boosting, Robustness, Ensemble methods

1. Introduction
The goal of robust regression methods is to provide reliable estimates for the unknown regression function even when the training data set may contain atypical observations. These “outliers” need not be “extreme” or aberrant values, but might simply be points following a different model from the one that applies to the majority of the data. It is well known that classical methods can provide seriously misleading results when trained on such heterogeneous or

*Corresponding author
Email addresses: xiaomeng.ju@stat.ubc.ca (Xiaomeng Ju), matias@stat.ubc.ca (Matías Salibián-Barrera)
Acknowledgments: This research is supported by Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.
contaminated data sets, and thus obtaining robust alternatives is of immediate practical importance.

In the robust regression literature much of the attention has been devoted to linear models, and a rich variety of proposals exists for them. For a review see, for example, Maronna et al. (2019). Fewer options are available for robust non-parametric regression methods, and generally they have not been developed as thoroughly as the linear ones. Among them we can mention: robust locally weighted regression (Cleveland, 1979; Wang and Scott, 1994), local M-estimators (Boente and Fraiman, 1989), local regression quantiles (Welsh, 1996), and the proposals in Härdle and Tsybakov (1988), Härdle (1990) and Oh et al. (2007). Unfortunately, when applied to problems with several explanatory variables, these methods suffer from the well known curse of dimensionality, requiring training sample sizes that grow exponentially with the number of covariates. An exception are the recently proposed robust estimators for additive models (Boente et al., 2017). However, selecting appropriate bandwidths for each of the components of an additive model can be computationally prohibitive when a moderate or large number of explanatory variables are available.

In this paper we study robust non-parametric regression estimators based on gradient boosting (Friedman, 2001). These ensemble methods are scalable to high-dimensional data, and typically require selecting fewer tuning parameters than additive models. Most robust boosting algorithms in the literature were designed for classification problems (Kégl, 2003; Rosset, 2005; Freund, 2009; Miao et al., 2015; Li and Bradic, 2018). Previous proposals to robustify boosting methods replaced the squared loss with the absolute value function, or Huber’s loss. Lutz et al. (2008) introduced several ways to robustify boosting, primarily focusing on linear regression. One of their methods (Robloss) can be extended to the scope of our study (nonlinear regression) by replacing the simple linear regression base learners with other types of base learners.

A different class of robust nonparametric regression methods are based on random forests. Roy and Larocque (2012) proposed simple variations of random forests that use the median to aggregate trees and make the tree splits. Li and Martin (2017) extended random forests from the squared loss to a broad family of loss functions, which leads to robust methods including: Huber forest, Tukey forest, and the quantile random forest which was also proposed by Meinshausen (2006).

Our main concern with these proposals is that they use robust loss functions that either may yield estimators with low efficiency (e.g. the $L_1$ loss) or require an auxiliary residual scale estimator (e.g. Huber’s and Tukey’s loss functions). For the latter, previous proposals suggested using in each step a robust scale estimator obtained with the residuals from the fit at the previous iteration (Friedman, 2001; Lutz et al., 2008). It is easy to see that this changing scale estimator may not work well, since the scale can be overestimated in early iterations and this might result in observations with large residuals not being considered outlying. In fact, our numerical experiments confirm that this is the case even in relatively simple settings. To address this problem, we propose a robust boosting method that directly minimizes a robust scale of the residu-
als, and hence does not need to compute an auxiliary residual scale estimator. Although in principle our approach can be used with any scale estimator, gradient boosting requires the gradient of the objective function. Hence, in this paper we focus on minimizing an M-estimator of scale, for which we can compute the corresponding gradient. This approach can be seen as an extension of S-estimators [Rousseeuw and Yohai 1984] to this class of non-parametric regression estimators. Moreover, this robust boosting estimator can be used (along with its associated robust residual scale estimator) as the initial fit for a boosting M-type estimator using Huber’s or Tukey’s loss. As in the case of linear models, this second stage is expected to result in a robust estimator with higher efficiency (less variability) than the S-estimator (Yohai 1987). Our proposal applies to practical situations where the proportion of potential outliers in the training and validation sets is unknown, and no parametric structure for the regression model is available. Furthermore, our approach can be used with relatively large numbers of explanatory variables.

The remainder of this paper is organized as follows. Section 2 introduces our proposed robust boosting regression estimator, and a variable importance score based on permutations. Section 3 reports the results of our simulation studies comparing our method with previously proposed robust boosting algorithms, while results obtained on benchmark data are discussed in Section 5. Finally, Section 6 summarizes our findings and conclusions.

2. Methodology

In this section we introduce our robust gradient boosting algorithm based on minimizing an M-estimator of the scale of the residuals. We also show how this fit can be further improved with a second gradient boosting step based on a bounded loss function. This second step reduces the variability of the fit without affecting its robustness. Finally, we discuss a variable importance method based on the permutation importance scores used with random forest (Breiman 2001).

2.1. SBoost: gradient boosting based on M-scale estimators

Consider a training data set \((x_i, y_i)\), where \(i \in I_{\text{train}}\), \(x_i \in \mathbb{R}^p\) and \(y_i \in \mathbb{R}\). The goal is to estimate the regression function \(F\) that relates the explanatory variables \(x\) to the response \(y\). The usual model behind this approach specifies that \(E(Y|X) = F(X)\). Gradient boosting assumes that \(F\) can be estimated with a function \(\hat{F}\) of the form:

\[
\hat{F}(x) = \sum_{t=1}^{T} \alpha_t h_t(x),
\]

where the functions \(h_t : \mathbb{R}^p \to \mathbb{R}\) (“base learners”) are typically chosen to be simple regressors such as decision trees with few splits, or linear functions. Often the base learners \(h_t\) are restricted to be functions of a single variable, which is akin to assuming an additive model.
Given a user-chosen loss function $L(a, b)$ (e.g. the squared loss $L(a, b) = (a - b)^2$), gradient boosting can be seen as a step-wise iterative algorithm to minimize the empirical risk

$$
\text{argmin}_F \sum_{i \in \mathcal{I}_{\text{train}}} L(y_i, F(x_i))
$$

over functions $F$ of the form (1). More specifically, let $n$ be the number of observations in the training set, $n = |\mathcal{I}_{\text{train}}|$, and consider the objective function above as a function of the $n$-dimensional vector $(F(x_1), \ldots, F(x_n))^\top$. At each step $t$ we compute the $i$-th coordinate of its gradient at the point obtained from the previous iteration $(\hat{F}_{t-1}(x_1), \ldots, \hat{F}_{t-1}(x_n))^\top$:

$$
g_{t,i} = \left. \frac{\partial L(y, b)}{\partial b} \right|_{b = \hat{F}_{t-1}(x_i)} , \quad i \in \mathcal{I}_{\text{train}},
$$

and form the gradient vector $g_t = (g_{t,1}, g_{t,2}, \ldots, g_{t,n})^\top$. Similar to the usual gradient descent algorithm that sequentially adds to the current point the negative gradient vector of the objective function, gradient boosting adds to the current function estimate an approximation to the negative gradient vector $(-g_t)$ using a base learner $h_t$. More specifically, at the $t$-th iteration $h_t$ is chosen to minimize

$$
\sum_{i \in \mathcal{I}_{\text{train}}} (h_t(x_i) + g_{t,i})^2,
$$

over members $h_t$ of the family of base learners. We then set

$$
\hat{F}_t(x) = \hat{F}_{t-1}(x) + \alpha_t h_t(x),
$$

where $\alpha_t$ is the optimal step size given by

$$
\alpha_t = \arg\min_\alpha \sum_{i \in \mathcal{I}_{\text{train}}} L(y_i, \hat{F}_{t-1}(x_i) + \alpha h_t(x_i)).
$$

Note that this algorithm requires an initial estimate $\hat{F}_0(x)$. When $L$ is the squared loss this initial estimator is usually taken to be the sample mean of the response variable in the training set. It is easy to see that this simple choice may not work well when there are atypical observations in the data set. In Section 2.1.1 below we present a better initialization approach for our setting.

Prior attempts to robustify boosting replaced the squared loss with the Huber loss, which requires the use of a preliminary scale estimator of the residuals. However, to estimate the scale of the residuals we need a robust regression estimator with which to compute the residuals. To avoid this problem we consider the following minimization problem instead:

$$
\hat{F} = \arg\min_F \hat{\sigma}_n(F),
$$
where $F$ is as in [1], and $\hat{\sigma}_n(F)$ is a robust estimator of the scale of the residuals $r_i(F) = y_i - F(x_i)$, $i \in I_{\text{train}}$. More specifically, in this paper we will focus on the case where $\hat{\sigma}_n$ is an M-estimator of scale given by

$$\frac{1}{|I_{\text{train}}|} \sum_{i \in I_{\text{train}}} \rho_0 \left( \frac{y_i - F(x_i)}{\hat{\sigma}_n(F)} \right) = \kappa,$$

where $\rho_0 : \mathbb{R} \to [0, +\infty)$ is a symmetric function around zero which controls the robustness and efficiency of the resulting estimator [Maronna et al., 2019]. In order to obtain a robust estimator, we use a bounded function $\rho_0$ in (2). For the associated scale estimator $\hat{\sigma}_n(F)$ to be consistent when the errors are Gaussian the constant $\kappa$ above needs to satisfy $\kappa = E_\phi[\rho_0(Z)]$, where $\phi$ denotes the standard normal distribution. This can always be computed once the function $\rho_0$ is selected. Note that if we take $\rho_0(u) = u^2$ this approach reduces to the usual boosting with the squared loss function.

In what follows we use a function in Tukey’s bisquare family as $\rho_0$ above, but our approach applies to any differentiable function $\rho_0$. Specifically, we choose

$$\rho_{\text{Tukey},c}(u) = \begin{cases} 1 - (1 - (\frac{|u|}{c})^2)^3 & \text{if } |u| \leq c \\ 1 & \text{if } |u| > c \end{cases}$$

For linear regression estimators the tuning constant $c > 0$ is generally selected to obtain maximum breakdown point, which is achieved when $c = 1.547$, which results in $\kappa = E_\phi[\rho_c(Z)] = 1/2$. We refer the interested reader to [Maronna et al., 2019] for details.

To compute the S-type boosting estimator, we follow the same approach used for gradient boosting, namely: at each step $t$ we calculate the gradient of the objective function (considered as a function of the $n$ fitted values), and approximate the negative gradient with a base learner. The $\ell$-th coordinate of the gradient at step $t$ is given by:

$$g_{t,\ell} = \frac{\partial \hat{\sigma}_n(y_1 - b_1, \ldots, y_n - b_n)}{\partial b_\ell} \bigg|_{b_\ell = \hat{F}_{t-1}(x_\ell)}, \quad \ell \in I_{\text{train}}.$$

The above can be computed explicitly by differentiating both sides of equation (2) with respect to $F(x_\ell)$, and noting that

$$0 = \sum_{i \in I_{\text{train}}} \frac{\partial}{\partial F(x_\ell)} \left[ \rho_0 \left( \frac{y_i - F(x_i)}{\hat{\sigma}_n(F)} \right) \right], \quad \ell \in I_{\text{train}}.$$

We have

$$0 = \sum_{i \in I_{\text{train}}} \psi_0 \left( \frac{y_i - F(x_i)}{\hat{\sigma}_n(F)} \right) \left( \frac{y_i - F(x_i)}{\hat{\sigma}_n(F)} \right) g_{t,\ell} - \psi_0 \left( \frac{y_i - F(x_i)}{\hat{\sigma}_n(F)} \right) \frac{1}{\hat{\sigma}_n(F)},$$
Algorithm 1: SBoost

\textbf{Input} : A data set \((x_i, y_i), i \in \mathcal{I}_{\text{train}}\)
The number of iterations \(T_1\)
The class of base learners \(\mathcal{H}\)

\textbf{Initialization} \(\hat{F}_0(x)\)

1. \textbf{for} \( t = 1 : T_1 \) \textbf{do}

2. \;

3. \;

4. \;

5. \;

6. \;

7. \;

8. \textbf{end}

\textbf{Output} : \(\hat{F}_{T_1}(x), \hat{\sigma}(\hat{F}_{T_1})\)

where \(\psi_0 = \rho_0\). Solving for \(g_{t, \ell}\) in the equation above we get

\[ g_{t, \ell} = C_t \psi_0 \left( \frac{y_\ell - \hat{F}_{t-1}(x_\ell)}{\hat{\sigma}_n(\hat{F}_{t-1})} \right), \]

where the constant \(C_t\) is

\[ C_t^{-1} = \sum_{i \in \mathcal{I}_{\text{train}}} \left[ \psi_0 \left( \frac{y_i - \hat{F}_{t-1}(x_i)}{\hat{\sigma}_n(\hat{F}_{t-1})} \right) \left( \frac{y_i - \hat{F}_{t-1}(x_i)}{\hat{\sigma}_n(\hat{F}_{t-1})} \right) \right]. \]

The resulting algorithm, which we call \textbf{SBoost}, is described in Algorithm [I]

2.1.1. The initial fit

Gradient boosting algorithms require an initial fit \(\hat{F}_0(x)\) to calculate the gradient vector for the first iteration. The classical gradient boosting algorithm is generally initialized with a constant fit \(\hat{F}_0(x) \equiv \alpha_0\) where \(\alpha_0\) solves

\[ \alpha_0 = \arg\min_{a \in \mathbb{R}} \sum_{i \in \mathcal{I}_{\text{train}}} L(y_i, a), \]

Since the loss function in Algorithm [I] is non-convex, the choice of initial fit for \textbf{SBoost} will typically be more important than for the usual gradient boosting with a squared loss function. A natural initial fit for a robust version of gradient boosting would be to take \(\alpha_0 = \text{median}(y_1, \ldots, y_n)\). However, we have found that this choice may not work well when the response variable includes a wide range of values. Intuitively the problem is that in those cases many “good”
observations may have large residuals $y_i - \alpha_0$ that result in a zero initial gradient $g_{1,i} = 0$, and subsequent iterations the algorithm fail to update $F(x_i)$. Instead, we recommend using a regression tree computed with the $L_1$ loss \cite{Breiman1984}. This tree, which we call LADTree, at each split minimizes the average absolute value of the residuals. This initial fit is expected to be robust to outliers in the training set; it is able to handle data of mixed types (quantitative, binary and categorical), and it is scalable to data with a large number of features.

2.2. RRBoost

Although our numerical experiments confirm the robustness of the SBoost fit \cite{Croux2019}, they also show a very low efficiency when the data do not contain outliers. Mimicking what is done to fix this issue in the case of S-estimators for linear regression, we propose to refine the SBoost estimator by using it as the initial fit for further gradient boosting iterations based on a bounded loss function that is closer to the squared loss function than $\rho_0$ in (2) (e.g. a Tukey’s bisquare function with a larger tuning constant). Moreover, in this second step we can use the scale estimator associated with the final SBoost fit ($\hat{\sigma}_n(\hat{F}_T)$).

This two-step procedure, which we call RRBoost can be summarized as follows:

- **Stage 1**: compute an $S$-type boosting estimator (SBoost) with high robustness but possibly low efficiency;
- **Stage 2**: compute an $M$-type boosting estimator initialized at the function and scale estimators obtained in Stage 1.

This approach solves the problem of many robust boosting proposals in the literature that require a preliminary residual scale estimator. Since it is known that highly robust regression S-estimators have low efficiency \cite{Hossjer1992}, the second step attempts to improve the efficiency of SBoost, similarly to what MM estimators do for linear regression models \cite{Yohai1987}.

The M-type boosting fit is given by

$$\hat{F} = \arg\min_F \sum_{i \in \mathcal{I}_{\text{train}}} \rho_1 \left( \frac{y_i - F(x_i)}{\hat{\sigma}_n} \right),$$

where $F$ is of the form (1), and $\hat{\sigma}_n = \hat{\sigma}(\hat{F}_T)$ is the residual scale estimator obtained from SBoost. In what follows we will use a Tukey’s bisquare function (3) for $\rho_1$ above, and set $c = 4.685$, which in the case of linear regression models yields 95\% asymptotic efficiency when the errors have a normal distribution \cite{Maronna2019}.

The gradient of the objective function above are easy to compute. At the
Algorithm 2: RRBoost algorithm

**Input**: A data set \((x_i, y_i), i \in I_{\text{train}}\)
- The number of stage 1 iterations \(T_1\)
- The number of stage 2 iterations \(T_2\)
- The class of base learners \(H\)

**Stage 1**: Run SBoost for \(T_1\) iterations and obtain:
\[
\hat{F}_{T_1}(x_i), \text{ and } \hat{\sigma}_n
\]

**Stage 2**:

\begin{itemize}
  \item \textbf{for } \(t = 1 : T_2\) \textbf{do}
  \item \(g_{t,i} = -\frac{1}{|I_{\text{train}}|\hat{\sigma}_n}\psi_1 \left( \frac{y_i - \hat{F}_{T_1+t-1}(x_i)}{\hat{\sigma}_n} \right)\)
  \item \(h_t = \arg\min_{h \in H} \sum_{i \in I_{\text{train}}} (g_{t,i} + h(x_i))^2\)
  \item \(\alpha_t = \arg\min_{\alpha} \sum_{i \in I_{\text{train}}} \rho_1 \left( \frac{|y_i - \hat{F}_{T_1+t-1}(x_i) - \alpha h_t(x_i)|}{\hat{\sigma}_n} \right)\)
  \item \(\hat{F}_{T_1+t}(x) = \hat{F}_{T_1+t-1}(x) + \alpha_t h_t(x)\)
\end{itemize}

**Output**: \(\hat{F}_{T_1+T_2}(x)\)

\(t\)-th iteration, its \(i\)-th coordinate is given by

\[
g_{t,i} = \frac{\partial}{\partial F(x_i)} \rho_1 \left( \frac{y_i - F(x_i)}{\hat{\sigma}_n} \right) \\
= -\frac{1}{\hat{\sigma}_n} \psi_1 \left( \frac{y_i - F(x_i)}{\hat{\sigma}_n} \right) , \quad i \in I_{\text{train}}.
\]

The algorithm for the second stage starts from the SBoost function estimator \(\hat{F}_{T_1}(x)\), and sequentially adds base learners \(h_1(x), \ldots, h_{T_2}(x)\) that approximate the corresponding vector of gradients at each step. The resulting RRBoost procedure is described in Algorithm 2.

### 2.3. Early stopping

The boosting algorithm is intrinsically greedy: at each step it attempts to maximize the reduction in the value of the loss function evaluated on the training set. Consequently, overfitting the training set at the expense of an increased generalization error (i.e. a poor performance on future data) is a practical concern. To mitigate this problem we propose to use an early stopping rule based on monitoring the performance of the ensemble on a validation set. This approach can be seen as a form of regularization.

We define the early stopping time of each stage of RRBoost as the iteration that achieves the lowest loss function value on a validation set (\(I_{\text{val}}\)). Let \(T_{1,\text{max}}\) and \(T_{2,\text{max}}\) be the maximum number of iterations allowed in RRBoost (Algorithm 2). In the first stage (SBoost), we refer to [2] and define the validation loss as

\[
L_{1,\text{val}}(t) = \hat{\sigma}_{\text{val}}(\hat{F}_t),
\]
where $\hat{\sigma}_{\text{val}}(\hat{F}_t)$ satisfies

$$\sum_{i \in I_{\text{val}}} \rho_0 \left( \frac{y_i - \hat{F}_t(x_i)}{\hat{\sigma}_{\text{val}}(\hat{F}_t)} \right) = \kappa.$$ 

The early stopping time for SBoost is

$$T_{1,\text{stop}} = \arg \min_{t \in \{1, \ldots, T_{1,\text{max}}\}} L_{1,\text{val}}(t).$$

In the second stage, referring to (4) we define the validation loss:

$$L_{2,\text{val}}(t) = \frac{1}{|I_{\text{val}}|} \sum_{i \in I_{\text{val}}} \rho_1 \left( \frac{y_i - \hat{F}_t(x_i)}{\hat{\sigma}_{\text{val}}(\hat{F}_{T_{1,\text{stop}}})} \right),$$

and the early stopping time

$$T_{2,\text{stop}} = \arg \min_{t \in \{T_{1,\text{max}}, \ldots, T_{2,\text{max}}\}} L_{2,\text{val}}(t).$$

In practice, when running boosting for $T_{1,\text{max}} + T_{2,\text{max}}$ iterations is too costly, one can terminate the boosting iterations when the validation error ceases to improve after several iterations.

2.4. Robust variable importance

We introduce robust variable importance as a by-product of RRBoost, which can be useful for selecting variables, interpreting strong predictors, and identifying variables that need to be measured to a great precision (Fisher et al., 2018). The variable importance suggested by Friedman (2001) for gradient boosting averages the improvement of squared error at each tree split at all iterations, but it cannot be generalized to arbitrary loss functions and is limited to tree base-leaners. Motivated by the permutation variable importance used in random forest (Breiman, 2001), we suggest a robust modification that applies to RRBoost.

Permutation importance measures the importance of a variable by permuting it in the training data and recording the decrease in prediction accuracy after the permutation. A feature is “important” if breaking its relationship with the response by shuffling its values increases the model error. Since our training data is contaminated, a robust prediction accuracy metric is needed to reduce the impact of outliers. We use trimmed root mean squared error and define the importance of variable $j$ as:

$$\text{VI}(x_j) = \sqrt{\frac{1}{|I_{\text{train}}|} \sum_{i \in I_{\text{train}}} (\hat{F}_{\pi_j}(x_i) - y_i)^2} - \sqrt{\frac{1}{|I_{\text{train}}|} \sum_{i \in I_{\text{train}}} (\hat{F}(x_i) - y_i)^2},$$
where \( \hat{F}(x) \) is fitted using the training data, and \( \hat{F}_{\pi_j}(x) \) is fitted using training data with the \( j \)th variable permuted. We trim the residuals that deviate at least 3 scale units from 0, where the scale unit is defined by the median absolute deviation (MAD) multiplied by a constant (1.438), which makes it an unbiased and consistent estimator of scale. Set \( \tilde{I}_{\text{train}} \) denotes the indices in the training set (\( I_{\text{train}} \)) that are not trimmed as outliers, which is defined as

\[
\tilde{I}_{\text{train}} = \{ i : i \in I_{\text{train}} \text{ and } |\hat{F}(x_i) - y_i| < 3\hat{\sigma}_r \},
\]

\[
\hat{\sigma}_r = 1.483 \text{MAD}(\hat{F}(x_i) - y_i, i \in I_{\text{train}}).
\]

3. Simulations

We performed extensive numerical experiments to assess the performance of RRBoost and compared it with that of other proposals in the literature. In particular, we focused on the accuracy and robustness of different boosting methods when the training and validation sets contain outliers, and also when no atypical observations are present.

3.1. Set up

Consider a data set \( D_n = \{(x_i, y_i), i = 1, \ldots, n\} \), consisting of predictors \( x_i \in \mathbb{R}^p \), where each coordinate \( x_{ij}, 1 \leq j \leq p \), is an independent \( \mathcal{U}(0,1) \) random variable. The responses \( y_i \in \mathbb{R} \) follow the model

\[
y_i = g(x_i) + C\epsilon_i, \quad i = 1, \ldots, n,
\]

where the errors \( \epsilon_i \) are independent from the explanatory variables \( x_i \), and \( C > 0 \) is a constant that controls the signal-to-noise ratio (SNR):

\[
\text{SNR} = \frac{\text{Var}(g(x))}{\text{Var}(C\epsilon)}.
\]

Given a function \( g \) and values of the predictors, the constant \( C \) that achieves a desired target SNR is

\[
C = \sqrt{\frac{\text{Var}(g(x))}{\text{SNR}}}
\]

In our experiments the function \( g \) was set to

\[
g(x) = \sum_{k=1}^{5} f_k(x),
\]

where \( f_1(x) = 2x_1 \), \( f_2(x) = -2x_2 \), \( f_3(x) = 8(x_3 - \frac{1}{2})^2 \), \( f_4(x) = \exp(x_4) \), and \( f_5(x) = 0.5\cos(8\pi x_5) \exp(2x_5) \). We considered the following error distributions:

- **Clean** (\( D_0 \)): \( \epsilon \sim N(0,0.1^2) \);
• **Symmetric gross errors** \((D_1)\): \(\epsilon \sim (1 - \alpha)N(0, 0.1^2) + \alpha(0.5N(20, 0.1^2) + 0.5N(-20, 0.1^2)), \alpha \in (0, 0.5)\); and

• **Asymmetric gross errors** \((D_2)\): \(\epsilon \sim (1 - \alpha)N(0, 0.1^2) + \alpha N(20, 0.1^2), \alpha \in (0, 0.5)\).

For the contaminated settings \(D_1\) and \(D_2\), we considered rates of contamination equal to 10% and 20% (which correspond to setting \(\alpha = 0.10\) and \(\alpha = 0.20\), respectively). We constructed training sets of size \(n = 300\) and validation sets of size \(n = 200\) following each of the cases above. To compare the performance of the different estimators, we also constructed a test set of size \(n = 1000\), which always follows \(D_0\).

The number of available explanatory variables was set to \(p = 10\) and \(p = 400\), the latter corresponding to a “high-dimensional” case where the size of the training set is smaller than the number of predictors \((n < p)\). The signal-to-noise ratio was set to \(\text{SNR} = 6\) when \(p = 10\) and \(\text{SNR} = 10\) for the \(p = 400\) case. The experiments were repeated 100 times, and we compared the following methods:

- **L2Boost**: gradient boosting with squared error loss \(\text{[Friedman 2001]}\);
- **LADBoost**: gradient boosting with absolute error loss \(\text{[Friedman 2001]}\);
- **MBoost**: gradient boosting with Huber’s loss \(\text{[Friedman 2001]}\);
- **Robloss**: Robloss boosting \(\text{[Lutz et al. 2008]}\);
- **SBoost**: SBoost (see Section 2.1) initialized with LADTree;
- **RRBoost**: RRBoost (see Section 2.2) initialized with LADTree.

The base learners for all methods under comparison were decision stumps (one-split regression trees).

We used the early stopping rules discussed in Section 2.3 with \(T_{1,\text{max}} = 500\) and \(T_{2,\text{max}} = 1000\). Similarly, for L2Boost, LADBoost, MBoost, and Robloss, we tracked their loss functions evaluated on the validation set \((L_{\text{val}}(t))\) and calculated the early stopping time \((T_{\text{stop}})\):

\[
T_{\text{stop}} = \arg\min_{t \in \{1, \ldots, T_{\text{max}}\}} L_{\text{val}}(t),
\]

where the maximum number of iterations \(T_{\text{max}} = 1500\).

To initialize RRBoost we considered LADTrees with depth 0, 1, 2, 3 and 4, and minimum number of observations per note set at 10, 20 or 30 (note that an LADTree of depth 0 corresponds to using the median of the responses as initial fit). Of the 13 different combinations we aimed to choose the one that performs the best on the validation set. As the validation set also contains outliers, we first fit the depth 0 tree and trimmed as potential outliers whose residuals deviate at least 3 scale units from 0. The observations that were not trimmed are denoted as:
\[ \hat{I}_{\text{val}} = \{i : i \in I_{\text{val}} \text{ and } |\hat{F}(x_i) - y_i| < 3\hat{\sigma}_{\text{val}}\}, \]

where

\[ \hat{\sigma}_{\text{val}} = 1.483\text{MAD}(\hat{F}(x_i) - y_i, i \in I_{\text{val}}) \]

We picked the one of the 13 combinations with the lowest trimmed absolute average deviation (AAD) on the validation set:

\[ \frac{1}{|I_{\text{val}}|} \sum_{i \in \hat{I}_{\text{val}}} |\hat{F}_{T_{\text{stop}}}(x) - y_i| . \]

All our simulations were run using the R programming environment (R Core Team, 2019). Regression trees were fit using the rpart package, including the LADTrees and the base learners. The code used in our experiments is publicly available on-line at https://github.com/xmengju/RRBoost.

3.2. Performance metrics

We compared different methods in terms of their predictive performance and variable selection accuracy. For predictive performance, we recorded the root mean squared error (RMSE) evaluated on the clean test set \((I_{\text{test}})\) at the early stopping time \((T_{\text{stop}})\):

\[ \text{RMSE}(T_{\text{stop}}) = \sqrt{\frac{1}{|I_{\text{test}}|} \sum_{i \in I_{\text{test}}} (\hat{F}_{T_{\text{stop}}}(x_i) - y_i)^2}. \]

For variable selection accuracy, we measured the proportion of variables recovered [Kazemitabar et al., 2017]. Specifically, let \(S\) be the set of indices of explanatory variables that were used to generate the data \((S = \{1, 2, \ldots, 5\})\). After ranking all \(p\) features using the robust imputation variable importance index, we recorded the proportion of true variables in the top \(|S|\) of the ordered list:

\[ \frac{1}{|S|} \left| \{j, \text{VI}(x_j) > \text{VI}(x_{(|S|)})\} \cap S \right| , \]

where \(\text{VI}(x_{(|S|)})\) is an order statistics, denoting the \(|S|\)th largest value of \(\text{VI}(x_1), ..., \text{VI}(x_p)\).

3.3. Results

Figure 1 and 2 compare the predictive performance of boosting methods under consideration. They show the boxplots of test root-mean-square error (RMSE) at early stopping times, where each boxplot was generated with the 100 results from independent runs of the experiment. Tables 1 and 2 show the summary statistics (mean, median, sd, and MAD) of these test RMSEs at early stopping times.

We find that, as expected, when there are no outliers in the training and validation sets, the performance of all methods are very similar, with the exception of SB, which is negatively affected by its low efficiency. Note that the subsequent M-step in RRboost completely fixes this problem.
Figure 1: Boxplots of RMSE on the test sets for 100 independent runs with $p = 10$ explanatory variables. The first panel corresponds to clean training sets. For the symmetrically and asymmetrically contaminated cases (panels (b) and (c), respectively), the yellow and blue boxplots correspond to 10% and 20% of outliers, respectively.

Table 1: Summary statistics of RMSEs on the test sets by L2Boost, MBoost, LADBoost, Robloss, SBoost, and RRBoost for clean (D0), symmetrically contaminated (D1), and asymmetrically contaminated (D2) data with $p = 10$; displayed in the form of: mean (SD) calculated from 100 independent runs of the experiment.
Figure 2: Boxplots of RMSE on the test sets for 100 independent runs with $p = 400$ explanatory variables. The first panel corresponds to clean training sets. For the symmetrically and asymmetrically contaminated cases (panels (b) and (c), respectively), the yellow and blue boxplots correspond to 10% and 20% of outliers, respectively.

|      | L2Boost | MBoost | LADBoost | Robloss | SBoost | RRBoost |
|------|---------|--------|----------|---------|--------|---------|
| D0   | 1.28 (0.07) | 1.61 (0.10) | 1.45 (0.12) | 1.56 (0.08) | 1.71 (0.11) | 1.28 (0.08) |
| D1 (10%) | 2.46 (0.24) | 4.78 (1.24) | 1.58 (0.12) | 2.00 (0.22) | 1.71 (0.13) | 1.32 (0.10) |
| D1 (20%) | 2.95 (0.36) | 9.00 (0.44) | 1.71 (0.12) | 3.56 (0.71) | 1.70 (0.11) | 1.37 (0.11) |
| D2 (10%) | 3.23 (0.33) | 5.25 (0.99) | 1.59 (0.13) | 2.15 (0.33) | 1.69 (0.12) | 1.33 (0.11) |
| D2 (20%) | 4.94 (0.37) | 9.05 (0.46) | 1.80 (0.13) | 6.11 (0.93) | 1.71 (0.11) | 1.38 (0.11) |

Table 2: Summary statistics of RMSEs on the test sets by L2Boost, MBoost, LADBoost, Robloss, SBoost, and RRBoost for clean (D0), symmetrically contaminated (D1), and asymmetrically contaminated (D2) data with $p = 400$; displayed in the form of: mean (SD) calculated from 100 independent runs of the experiment.
Table 3: Fractions of variables recovered by L2Boost, MBoost, LADBoost, Robloss, and RRBoost for clean (D0), symmetrically contaminated (D1), and asymmetrically contaminated (D2) data with $p = 10$; displayed in the form of: mean (SD) calculated from 100 independent runs of the experiment.

|        | L2Boost | MBoost | LADBoost | Robloss | RRBoost |
|--------|---------|--------|----------|---------|---------|
| D0     | 1(0)    | 1(0)   | 1(0.02)  | 1(0)    | 1(0)    |
| D1(10%)| 0.29(0.23) | 0.7(0.19) | 1(0) | 0.97(0.07) | 1(0) |
| D1(20%)| 0.28(0.25) | 0.57(0.18) | 0.99(0.04) | 0.83(0.15) | 1(0) |
| D2(10%)| 0.34(0.24) | 0.64(0.17) | 1(0.02) | 0.93(0.11) | 1(0) |
| D2(20%)| 0.23(0.17) | 0.59(0.15) | 0.98(0.06) | 0.66(0.16) | 1(0) |

When the number of predictors is $p = 10$, the performances of L2Boost, MBoost, and Robloss seriously deteriorate as the percentage of contamination increases from 10% to 20%, while RRBoost achieves the lowest average test RMSE among all methods, and its performance is remarkably stable for different proportions of contamination.

For the high-dimensional setting with $p = 400$, the results in Figure 2 show similar patterns to the ones for $p = 10$. RRBoost performs very similarly to the standard gradient boosting when the training and validation sets do not contain outliers, and outperforms other methods when the data contain outliers. It is interesting to note that robust boosting methods using Huber’s loss function (MBoost and Robloss) perform worse than gradient boosting with squared loss (L2Boost) in many contaminated settings. One explanation for the behaviour of MBoost with 20% of outliers is that at each iteration $t$, Friedman (2001) suggested setting the tuning constant of the loss function at the 90% quantile of the residuals $\{y_i - \hat{F}_t(x_i)\}_{i \in \mathcal{X}_{\text{train}}}$. It is not immediately clear how to address this issue without assuming that the proportion of outliers is known.

We also calculated variable importance indices for each independent run of the experiment. The resulting fractions of variables recovered (3.2) for the cases $p = 10$ and $p = 400$ are reported in Tables 3 and 4, respectively. We note that for $p = 10$, RRBoost and LADBoost recovered almost all variables for clean and contaminated data, whereas the other boosting methods (especially L2Boost and MBoost) recovered much less variables when trained with contaminated data compared to clean data. In the high-dimensional case (Table 4), RRBoost also performs well (with at least 90% of the variables recovered), whereas variable selection in contaminated settings appears to be more difficult for the other methods. In particular, L2Boost and MBoost almost never selected the true variables, considering their fraction of variables recovered are less than 5% on average.

4. Real Data

We evaluated the performance of our proposed algorithm on real-world data sets, where we expect to find complex correlation structures among the explanatory variables. We considered 6 data sets with different combinations of number
Table 4: Fractions of variables recovered by L2Boost, MBoost, LADBoost, Robloss, and RRBoost for clean (d0), symmetrically contaminated (d1), and asymmetrically contaminated (d2) data with \( p = 400 \); displayed in the form of: mean (SD) calculated from 100 independent runs of the experiment.

|        | L2Boost | MBoost | LADBoost | Robloss | RRBoost |
|--------|---------|--------|----------|---------|---------|
| D0     | 0.99(0.03) | 0.99(0.04) | 0.9(0.15) | 0.99(0.06) | 0.98(0.05) |
| D1(10%)| 0.02(0.07) | 0.26(0.26) | 0.77(0.2) | 0.85(0.16) | 0.98(0.07) |
| D1(20%)| 0.01(0.05) | 0.03(0.07) | 0.5(0.27) | 0.45(0.24) | 0.95(0.1) |
| D2(10%)| 0.02(0.06) | 0.21(0.22) | 0.77(0.21) | 0.84(0.14) | 0.98(0.06) |
| D2(20%)| 0.02(0.05) | 0.05(0.09) | 0.5(0.28) | 0.2(0.2) | 0.94(0.1) |

Table 5: Description of the real data sets included in our study.

| Name   | Size \((n)\) | Dimension \((p)\) | Source                        |
|--------|--------------|-------------------|-------------------------------|
| airfoil| 1503         | 5                 | UCI (Brooks et al., 1989)     |
| abalone| 4177         | 7                 | UCI (Nash et al., 1994)       |
| wage   | 3000         | 8                 | ISLR R package (James et al., 2013) |
| nir    | 103          | 94                | pls R package (Wehrens and Mevik, 2007) |
| tecator| 215          | 100               | caret R package (Kuhn, 2019)  |
| glass  | 180          | 486               | Serneels et al. (Serneels et al., 2005) |

of cases and explanatory variables. Their main characteristics are summarized in Table 5. To compare the prediction power of different boosting algorithms we follow the setting in Jung et al. (2016). Each data set was split into a training set (composed of 60% of the data), a validation set (20% of the data) and a test set with the remaining 20%. We ran the boosting algorithms on the training sets, and used the validation sets to select an early stopping time. The prediction performances are evaluated on the test sets.

To study the behaviour of the algorithms when the data may be contaminated, we randomly added 20% of outliers to the training and validation sets as follows:

\[ y_i = y^*_i + C\epsilon_i, \]

where \( y^*_i \) are the original responses, \( \epsilon_i \) are random errors, and \( C > 0 \) is a constant chosen to achieve a desired signal-to-noise ratio (SNR). As before, we use

\[ C = \sqrt{\frac{S^2(y^*)}{SNR}}, \]

where \( S^2(y^*) \) is the sample variance of the response variable. We set SNR = 10 for the high dimensional glass data and SNR = 6 for the other data sets. For the errors \( \epsilon_i \) we considered two contamination settings:

- **symmetric contamination:**
  \[ \epsilon \sim 0.5N(20,0.1^2) + 0.5N(-20,0.1^2) \] for 20% of the data;

- **asymmetric contamination:**
  \[ \epsilon \sim N(20,0.1^2) \] for 20% of the data.
Predictive performance was measured with the average absolute deviance (AAD) of residuals:

\[
\frac{1}{|\mathcal{I}_{\text{test}}|} \sum_{i \in \mathcal{I}_{\text{test}}} |\hat{F}_{T_{\text{stop}}}(x) - y_i|
\]

at the early stopping time \(T_{\text{stop}}\). We used the same base-learners and number of iterations as in Section 3. In order to reduce the potential variability induced by the random partition into training, validation and test sets, we repeated the experiment 50 times with different random splits. The summary statistics for clean, symmetrically contaminated and asymmetrically contaminated data sets are displayed in Tables 6 to 8.

|                  | L2Boost   | MBoost    | LADBoost  | Robloss   | RRBoost   |
|------------------|-----------|-----------|-----------|-----------|-----------|
| airfoil          | 3.57(0.16)| 3.53(0.15)| 3.48(0.17)| 3.49(0.16)| 3.43(0.25)|
| abalone          | 1.62(0.04)| 1.6(0.04) | 1.69(0.07)| 1.6(0.05) | 1.58(0.05)|
| wage             | 23.49(1.07)| 23.08(1.13)| 23.05(1.13)| 23.03(1.16)| 23.08(1.18)|
| nir              | 3.39(0.66)| 3.28(0.53)| 3.74(0.73)| 3.25(0.6) | 3.48(0.74)|
| tecator          | 4.48(0.72)| 4.51(0.67)| 6.38(0.92)| 4.56(0.71)| 4.86(0.9) |
| glass            | 0.23(0.07)| 0.29(0.08)| 0.27(0.11)| 0.28(0.06)| 0.28(0.12)|

Table 6: Average absolute deviance (AAD) of residuals for L2Boost, MBoost, LADBoost, Robloss, and RRBoost with clean data; displayed in the form of: mean (SD) calculated from 50 random data splits.

|                  | L2Boost   | MBoost    | LADBoost  | Robloss   | RRBoost   |
|------------------|-----------|-----------|-----------|-----------|-----------|
| airfoil          | 4.96(0.41)| 5.03(0.5) | 3.53(0.19)| 3.93(0.2) | 3.26(0.23)|
| abalone          | 2.07(0.11)| 2.11(0.13)| 1.7(0.07) | 1.94(0.14)| 1.6(0.05) |
| wage             | 27.42(1.55)| 27.9(1.81)| 23.08(1.2) | 23.89(1.31)| 23.03(1.22)|
| nir              | 10.84(2.86)| 16.84(3.51)| 4.59(1.22)| 16.02(3.7) | 3.85(0.81)|
| tecator          | 9.79(1.98)| 16.53(3.49)| 6.55(0.94)| 15.55(3.67)| 5.06(0.83)|
| glass            | 0.77(0.39)| 1.74(0.3) | 0.29(0.12)| 1.45(0.33)| 0.31(0.14)|

Table 7: Average absolute deviance (AAD) of residuals for L2Boost, MBoost, LADBoost, Robloss, and RRBoost with symmetrically contaminated data; displayed in the form of: mean (SD) calculated from 50 random data splits.

As expected, Table 6 shows that when the data do not contain outliers the difference between RRBoost and L2Boost is not significant. However, when outliers were introduced in the data, Tables 7 and 8 indicate that LADBoost and RRBoost generally perform better than the other methods. In particular, when the data sets were asymmetrically contaminated, RRBoost had the best performance in terms of mean AAD for most data sets.

5. Conclusion

In this paper we propose a novel robust boosting estimator (RRBoost) which combines S-type and an M-type boosting estimators. This approach allows us
to use bounded loss functions, which are known to provide strong protection against outliers. As expected, our experiments show that outliers, particularly when they are asymmetrically distributed, can affect significantly the performance of the classical L2Boost algorithm. We also found that our proposed RRBoost can be much more robust than other prior robust boosting methods, while behaving very similarly to L2Boost when the data do not contain atypical observations. In particular, the second stage of RRBoost significantly improves the prediction accuracy of the initial SBoost fit. Using a permutation-based variable importance ranking we show that in our experiments RRBoost achieved the best variable selection accuracy across the different contamination settings.

References

Boente, G. and Fraiman, R. (1989). Robust nonparametric regression estimation. *Journal of Multivariate Analysis*, 29:180–198.

Boente, G., Martínez, A., and Salibián-Barrera, M. (2017). Robust estimators for additive models using backfitting. *Journal of Nonparametric Statistics*, 29(4):744–767.

Breiman, L. (1984). *Classification and regression trees*. Routledge.

Breiman, L. (2001). Random forests. *Machine learning*, 45(1):5–32.

Brooks, T. F., Pope, D. S., and Marcolini, M. A. (1989). Airfoil self-noise and prediction. *NASA reference publication*.

Cleveland, W. S. (1979). Robust locally weighted regression and smoothing scatterplots. *Journal of the American statistical association*, 74(368):829–836.

Fisher, A., Rudin, C., and Dominici, F. (2018). All models are wrong but many are useful: Variable importance for black-box, proprietary, or misspecified prediction models, using model class reliance.

Freund, Y. (2009). A more robust boosting algorithm.
Friedman, J. H. (2001). Greedy function approximation: a gradient boosting machine. *Annals of statistics*, pages 1189–1232.

Härdle, W. (1990). *Applied Nonparametric Regression*, volume 19 of *Econometric Society Monographs*. Cambridge University Press, Cambridge.

Härdle, W. and Tsybakov, B. (1988). Robust nonparametric regression with simultaneous scale curve estimation. *Annals of Statistics*, 16:120–135.

Hössjer, O. (1992). On the optimality of s-estimators. *Statistics and Probability Letters*, 14(5):413–419.

James, G., Witten, D., Hastie, T., and Tibshirani, R. (2013). *ISLR: Data for an introduction to statistical learning with applications in R*. R package.

Jung, Y., Lee, S. P., and Hu, J. (2016). Robust regression for highly corrupted response by shifting outliers. *Statistical Modelling*, 16(1):1–23.

Kazemitabar, J., Amini, A., Bloniarz, A., and Talwalkar, A. S. (2017). Variable importance using decision trees. In *Advances in Neural Information Processing Systems*, pages 426–435.

Kégl, B. (2003). Robust regression by boosting the median. In *Learning Theory and Kernel Machines*, pages 258–272. Springer.

Kuhn, M. (2019). *caret: Classification and Regression Training*. R package.

Li, A. H. and Bradic, J. (2018). Boosting in the presence of outliers: adaptive classification with nonconvex loss functions. *Journal of the American Statistical Association*, 113(522):660–674.

Li, A. H. and Martin, A. (2017). Forest-type regression with general losses and robust forest. In *International Conference on Machine Learning*, volume 70, pages 2091–2100.

Lutz, R. W., Kalisch, M., and Bühlmann, P. (2008). Robustified l2 boosting. *Computational Statistics & Data Analysis*, 52(7):3331–3341.

Maronna, R. A., Martin, R. D., Yohai, V. J., and Salibián-Barrera, M. (2019). *robust statistics: theory and methods (with r)*. John Wiley & Sons.

Meinshausen, N. (2006). Quantile regression forests. *Journal of Machine Learning Research*, 7(Jun):983–999.

Miao, Q., Cao, Y., Xia, G., Gong, M., Liu, J., and Song, J. (2015). Rboost: label noise-robust boosting algorithm based on a nonconvex loss function and the numerically stable base learners. *IEEE transactions on neural networks and learning systems*, 27(11):2216–2228.
Nash, W. J., Sellers, T. L., Talbot, S. R., Cawthorn, A. J., and Ford, W. B. (1994). The population biology of abalone (haliotis species) in tasmania. i. blacklip abalone (h. rubra) from the north coast and islands of bass strait. *Sea Fisheries Division, Technical Report*, 48.

Oh, H.-S., Nychka, D., and Lee, T. (2007). The role of pseudo data for robust smoothing with applications to wavelet regression. *Biometrika*, 94(4):893–904.

R Core Team (2019). *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria.

Rosset, S. (2005). Robust boosting and its relation to bagging. In *Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining*, pages 249–255. ACM.

Rousseeuw, P. and Yohai, V. (1984). Robust regression by means of s-estimators. In *Robust and nonlinear time series analysis*, pages 256–272. Springer.

Roy, M.-H. and Larocque, D. (2012). Robustness of random forests for regression. *Journal of Nonparametric Statistics*, 24(4):993–1006.

Serneels, S., Croux, C., Filzmoser, P., and Van Espen, P. J. (2005). Partial robust m-regression. *Chemometrics and Intelligent Laboratory Systems*, 79(1-2):55–64.

Wang, F. T. and Scott, D. W. (1994). The l1 method for robust nonparametric regression. *Journal of the American Statistical Association*, 89(425):65–76.

Wehrens, R. and Mevik, B.-H. (2007). *The pls package: principal component and partial least squares regression in R*. R package.

Welsh, A. (1996). Robust estimation of smooth regression and spread functions and their derivatives. *Statistica Sinica*, 6:347–366.

Yohai, V. J. (1987). High breakdown-point and high efficiency robust estimates for regression. *The Annals of Statistics*, 15(2):642–656.