Understanding Neural Networks via Rule Extraction

Rudy Setiono and Huan Liu *
Department of Information Systems and Computer Science
National University of Singapore
Kent Ridge, Singapore 0511
{rudys,liuh}@iscs.nus.sg

Abstract

Although backpropagation neural networks generally predict better than decision trees do for pattern classification problems, they are often regarded as black boxes, i.e., their predictions are not as interpretable as those of decision trees. This paper argues that this is because there has been no proper technique that enables us to do so. With an algorithm that can extract rules1, by drawing parallels with those of decision trees, we show that the predictions of a network can be explained via rules extracted from it, thereby, the network can be understood. Experiments demonstrate that rules extracted from neural networks are comparable with those of decision trees in terms of predictive accuracy, number of rules and average number of conditions for a rule; they preserve high predictive accuracy of original networks.

1 Introduction

Researchers [Dietterich et al., 1990; Quinlan, 1994; Shavlik et al., 1991] have compared experimentally the performance of learning algorithms of decision trees and neural networks (NNs). A general picture of these comparisons is that: (1) Backpropagation (an NN learning method) usually requires a great deal more computation; (2) the predictive accuracy of both approaches is roughly the same, with backpropagation often slightly more accurate [Quinlan, 1994]; and (3) symbolic learning (decision trees induction) can produce interpretable rules while networks of weights are harder to interpret [Shavlik et al., 1991]. In effect, a neural network is widely regarded as a black box due to the fact that little is known about how its prediction is made.

Our view is that this is because we are not equipped with proper techniques to know more about how a neural network makes a prediction. If we can extract rules from neural networks as generating rules from decision trees, we can certainly understand better how a prediction is made. In addition, rules are a form of knowledge that can be easily verified by experts, passed on and expanded. Some recent works [Fu, 1994; Saito and Nakano, 1988; Towell and Shavlik, 1993] have shown that rules can be extracted from networks. These algorithms are search-based methods that have exponential complexity. Subsets of incoming weights that exceed the bias on a unit are searched. Such sets are then rewritten as rules. To simplify the search process, some assumptions are made. One assumption is that the activation of a unit is either very close to 1 or very close to 0. This can restrict the capability of the network since when the sigmoid transfer function is used as the activation function, the activation of a unit can have any value in the interval (0,1).

In this paper, a novel way to understand a neural network is proposed. Understanding a neural network is achieved by extracting rules with a three-phase algorithm: first, a weight-decay backpropagation network is built so that important connections are reflected by their bigger weights; second, the network is pruned such that insignificant connections are deleted while its predictive accuracy is still maintained; and last, rules are extracted by recursively discretizing the hidden unit activation values. By drawing parallels with the rules generated from decision trees, we show that networks can be interpreted by the extracted rules; the rules in general preserve the accuracy of the networks; and they also explain how a prediction is made.

2 A Three-Phase Algorithm

A standard three layer feedforward network is the base of the algorithm. Weight decay is implemented while backpropagation is carried out. After the network is pruned, its hidden units activation values are discretized. Rules are extracted by examining the discretized activation values of the hidden units. The algorithm is described in steps below.

2.1 Backpropagation with Weight Decay

The basic structure of the neural network in this work is a standard three-layer feedforward network, which consists of an input layer, I, a hidden layer, H, and an output...
layer, $O$. The number of input units corresponds to the dimensionality of the examples of a classification problem. The number of output units is determined by the number of classes in the data. The number of hidden units depends on the problem in hand. Two approaches to determine a suitable number of hidden units have been described in the literature. The first approach begins with a minimal number of hidden units, one or two, and more hidden units are added as they are needed to increase the accuracy of the network. The second approach begins with an oversized network and removes redundant connections in the network by pruning. In the process, hidden units that are not connected to any input units or/and output units can be removed as well. We adopt the second approach since we are also interested in removing irrelevant input units.

Given an $n$-dimensional example $x^i$, $i \in \{1,2,\ldots,k\}$ as input, let $w^{m}_{p}$ be the weight for the connection from input unit $i$, $i \in \{1,2,\ldots,n\}$ to hidden unit $m$, $m \in \{1,2,\ldots,h\}$ and $v^{m}_{p}$ be the weight from hidden unit $m$ to output unit $p$, $p \in \{1,2,\ldots,o\}$, the $p$th output of the network for example $x^i$ is obtained by computing

$$S^i_p = \sigma (\sum_{m=1}^{h} a^m v^{m}_{p}), \text{ where}$$

$$a^m = \delta \left( \sum_{l=1}^{n} x^i_l w^{m}_{l} \right), \delta(x) = (e^{x} - e^{-x})/(e^{x} + e^{-x}).$$

The target output for an example $x^i$ that belongs to class $C_j$ is an $o$-dimensional vector $t^i$, where $t^i_p = 0$ if $p \neq j$ and $t^i_j = 1$, $j, p = 1,2,\ldots,o$. The backpropagation algorithm is applied to update the weights $(w, v)$ and minimize the following function:

$$F(w, v) = F(w, v) + P(w, v),$$

where $F(w, v)$ is the cross entropy function:

$$F(w, v) = -\sum_{i=1}^{k} \sum_{j=1}^{o} (t^i_j \log S^i_j - (1 - t^i_j) \log(1 - S^i_j)).$$

and $P(w, v)$ is a penalty term used for weight decay:

$$P(w, v) = \epsilon_1 \left( \sum_{m=1}^{h} \sum_{l=1}^{n} \beta(w^{m}_{l})^2 + \sum_{m=1}^{h} \sum_{p=1}^{o} \beta(v^{m}_{p})^2 \right),$$

$$+ \epsilon_2 \left( \sum_{m=1}^{h} \sum_{l=1}^{n} (w^{m}_{l})^2 + \sum_{m=1}^{h} \sum_{p=1}^{o} (v^{m}_{p})^2 \right).$$

Using this penalty function, we have been able to obtain networks with less number of connections than the previously reported for many learning problems. Details of the comparison and the choice of the parameter values ($\epsilon_1, \epsilon_2,$ and $\beta$) are given in [Setiono, 1995].

2.2 Network Pruning

A neural network pruning algorithm is briefly described below.

Neural network pruning algorithm

1. Let $\eta_1$ and $\eta_2$ be positive scalars such that $\eta_1 + \eta_2 < 0.5$.
2. Pick a fully connected network. Train this network until a predetermined accuracy rate is achieved and for each correctly classified example the condition

$$\max_{p} |e^i_p| = \max_{p} |S^i_p - t^i_p| \leq \eta_1,$$

where $\eta_1 \in [0,0.5]$, is satisfied.
3. Let $(w, v)$ be the weights of this network. For each $w^{m}_p$, if

$$\max_{p} |w^{m}_p v^{m}_p| \leq 4\eta_2,$$

then remove $w^{m}_p$ from the network.
4. For each $v^{m}_p$, if

$$\max_{p} |v^{m}_p| \leq 4\eta_2,$$

then remove $v^{m}_p$ from the network.
5. If no weight satisfies condition (4) or condition (5), then remove $w^{m}_p$ with the smallest product $\max_p |w^{m}_p v^{m}_p|$.
6. Retrain the network. If classification rate of the network falls below an acceptable level, then stop. Otherwise, go to Step 3.

This pruning algorithm removes the connections of the network according to the magnitudes of their weights (4 and 5). As our eventual goal is to get a set of simple rules that describe the classification process, it is important that all unnecessary connections be removed. In order to remove as many connections as possible, it is therefore imperative that the weights be prevented from taking values that are too large. At the same time, weights of irrelevant connections should be encouraged to converge to zero.

2.3 Rule Extraction

When network pruning is completed, the network contains only those salient connections. Nevertheless, rules are not readily extractable because the hidden unit activation values are continuous. The discretization of these values paves the way for rule extraction. The following algorithm discretizes the activation values (many clustering algorithms can be used for this purpose).

Discretizing Hidden Unit Activation Values by Clustering

For each hidden unit,
1. Let $\epsilon \in (0,1)$,
2. Start with activation value $a_{1}$ of the first example in the training set,
3. Cluster activation values $(a_{i})$ for the remaining examples if $|a_{i} - a_{1}| < \epsilon$,
4. Represent this cluster’s activation value by the average of the activation values in the cluster;
5. Select next $a_{n}$, repeat 3 and 4 for clustering until all activation values are clustered.
When the clustering is done, the network's accuracy is checked to see if it drops or not. A very small $\epsilon$ can guarantee that the network with discretized activation values is as accurate as the original network with continuous activation values. So if it's accuracy does not drop and there are still many discrete values, clustering can be performed again with a larger $\epsilon$. Otherwise, $\epsilon$ should be reduced to a smaller value.

After network pruning and activation value discretization, rules can be extracted by examining the possible combinations in the network outputs (explained in detail in Section 3.2). The actual rule extraction is done by an algorithm that generates 100% accurate rules [Liu, 1995]. However, when there are still too many connections (e.g., more than 7) between a hidden unit and input units, the extracted rules may not be easy to understand. Another three layer feedforward subnetwork may be employed to simplify rule extraction for the hidden unit. This subnetwork is trained in the same ways as is the original network, but in a reduced scale: the number of output units is the number of discrete values of the hidden unit, while the input units are those connected to the hidden unit in the original network. Examples are grouped according to their discretized activation values. Given $d$ discrete activation values $D_1, D_2, \ldots, D_d$, all examples with activation values equal to $D_j$ are given a $d$-dimensional target value of all zeros except for one 1 in position $j$. A new hidden layer is introduced for this subnetwork and it is then trained, pruned, and the activation values of its hidden units are discretized for rule extraction. If necessary, another subnetwork is created until the number of connection is small enough or the new subnetwork cannot simplify the connections between the inputs and the hidden unit at the higher level. The creation of subnetworks is rarely needed. For example, in our experiments, it was only used for the Splice-junction problem.

### 3 Experiments and Results

In this section, we describe the datasets and representations used in experiments. A detailed example is given to show how the three-phase algorithm is applied to extracting rules. Summary of the results on all datasets are given with a comparison to those produced by the decision tree induction methods. Understanding a neural network is achieved by being able to explain, based on the rules, how each prediction is made in parallel with understanding a decision tree by having rules generated from it [Quinlan, 1993].

#### 3.1 Datasets and Representations

Three datasets used are: 1. Iris - a classic dataset introduced by R.A. Fisher [1936]; 2. Breast Cancer - a widely tested real-world dataset for the Wisconsin Breast Cancer diagnosis; and 3. Splice-junction - a dataset used in splice-junction determination originally described by Noordewier et al [1991]. The datasets are obtainable from the University of California Irvine data repository for machine learning (via anonymous ftp from ics.uci.edu). The summary of these datasets, their representations, and how each dataset is used in experiments are given below.

- **Iris** - the dataset contains 50 examples each of the classes Iris setosa, Iris versicolor, and Iris virginica (species of iris). Each example is described using four numeric attributes ($A_1, A_2, A_3$, and $A_4$): sepal-length, sepal-width, petal-length, and petal-width. Since each attribute takes a continuous value, the ChiMerge algorithm proposed by Kerber [1992] was reimplemented to discretize attribute values. The thermometer code [Smith, 1993] is used to binarize the discretized values; 16, 9, 7, and 6 inputs (discrete values) for $A_1, A_2, A_3$, and $A_4$, respectively. With 1 input for bias, there are total 39 inputs and three outputs. Examples in odd positions in the original dataset form the training set and the rest are for testing as was done in [Fu, 1994].

- **Breast Cancer** - the dataset consists of 699 examples, of which 458 examples are classified as benign, and 241 are malignant. 50% examples of each class were randomly selected (i.e., 229 benign and 121 malignant examples) for training, the rest for testing in the experiments. Each example is described by 9 attributes, each attribute takes an ordinal integer from 1 to 10 (10 values). Due to the ordinal nature, the thermometer code is used again to code each attribute value. Ten inputs correspond to 10 values of each attribute with all 10 inputs representing value 10, the rightmost input on for value 1, and the two rightmost inputs on for value 2, etc.

- **Splice-junction** - the data set contains 3175 examples, approximately 25% are exon/intron boundaries (EI), 25% are intron/exon boundaries (IE), and remaining 50% are neither (N). Each example consists of a 60-nucleotide-long DNA sequence categorized with EI, IE or N. Each of these 60 attributes takes one of the four values: G, T, C or A that are coded as 1000, 0100, 0010, and 0001, respectively. The class values (EI, IE, N) are similarly coded as 100, 010, and 001, respectively. For the results presented here, the training data set consists of 1006 examples while the testing data set consists of all 3175 examples.

#### 3.2 A Detailed Example – Iris Data Classification

This example shows in detail how rules are extracted from a pruned network. In the experiment, 100 fully connected neural networks were used as the starting networks. Each of these networks consists of 39 input units, 3 hidden units and 3 output units. These networks were trained with initial weights that had been randomly generated in the interval $[-1, 1]$. Each of the trained networks was pruned until its accuracy on the training data dropped below 95%. The weights and topology of networks with the smallest number of connections and an accuracy rate of more than 97% were saved for possible rule extraction. The results of these experiments are summarized in Table 1 where we list the average number of connections in the pruned networks and their

---

2Another 15 examples in the original dataset contain invalid values so these examples are not included in experiment.
average accuracy rates on the training data and the testing data. Statistics in the second column of this table were obtained from 100 pruned networks, all of which have accuracy rates on the training data of at least 95%. In the third column, the figures were obtained from 100 pruned networks with accuracy of at least 97% on the training data.

One of the smallest pruned networks is depicted in Figure 1. It has only two hidden units and a total of 8 connections with 98.67% accuracy on the training set and 97.33% on the testing set. We ran the clustering algorithm of Section 2.3 on this network and found only two discrete values are needed at each of the two hidden units to maintain the same level of accuracy on the training data. At hidden unit 1, 48 of 75 training examples have activation values equal to 0, and the remaining 27 have activation values equal to 1. At hidden unit 2, the activation value of 25 examples is 1 and the activation value of the remaining 50 examples is -0.5. Since we have two activation values at each of the two hidden units, four different outcomes at the output units are possible (Table 2). From this table, it is clear that an example will be classified as Iris setosa as long as its activation value at the second hidden unit is equal to 1. Otherwise, the example is classified as Iris versicolor provided that its first hidden unit activation value $H_{l1} = 0$. The default class will then be Iris virginica.

As seen in Figure 1, only two inputs, $L_{31}$ and $L_{39}$, determine the activation values of the second hidden unit, $H_2$. However, since $L_{39}$ is 1 for all the training data, $H_2$ is effectively determined by $L_{31}$. Since the weights of the arcs connecting input units 31 and 39 to the second hidden unit are -5.4 and 4.8 respectively, it is easy to conclude that if $L_{31} = 0$, then $H_2$ is 1, otherwise, $H_2$ is -0.52. This implies that an example will be classified as Iris setosa only if $L_{31} = 0$ (hence $H_2$ is 1).

The activation value of the first hidden unit, $H_{l1}$, depends only on $L_{26}$ and $L_{34}$. The weights of the arcs connecting input units 26 and 34 to the first hidden unit are 5.1 and 8.1, respectively, hence $H_{l1} = 0$ if and only if $L_{26} = L_{34} = 0$. Other input combinations will yield value 1 for $H_{l1}$. Hence, an example with $L_{31} = 1$, $L_{26} = L_{34} = 0$ will be classified as Iris versicolor.

With the thermometer coding scheme used for the input, a complete set of rules can be easily obtained in terms of the original attributes of the iris data set. The accuracy of this rule set is summarized in Table 3:

**Table 3:** Accuracy of NN rules and DT rules on the training and testing data.

### NN Rules

**Rule 1:** If Petal-length $\leq 1.9$ then Iris setosa

**Rule 2:** If Petal-length $\leq 4.9$ and Petal-width $\leq 1.6$ then Iris versicolor

**Default Rule:** Iris virginica.

For reference, the rule set (DT Rules) generated by C4.5 rules (based on a decision tree method but generate more concise rules than the tree itself) is included here:

### DT Rules

**Rule 1:** If Petal-length $\leq 1.9$ then Iris setosa

**Rule 2:** If Petal-length $> 1.9$ and Petal-width $\leq 1.6$ then Iris versicolor

**Rule 3:** If Petal-width $> 1.6$ then Iris virginica

**Default Rule:** Iris setosa.

### 3.3 Comparisons

In this section, parallels are drawn between rules extracted from both neural networks and decision trees

---

*The rules are fired in a top-down and left-to-right fashion.*
(NN rules vs. DT rules). Understandability is partly defined as being explicable in the sense that a prediction can be explained in terms of inputs (or attribute values). Choosing to compare NN rules with DT rules is due to the fact that DT rules are considered best understandable among the available choices. A rule in discussion consists of two parts: the if-part is made of a conjunction of conditions, and the then-part specifies a class value. The conditions of a rule are in forms of “A_i = V_j”, i.e., attribute A_i takes value V_j. When a rule is fired, a prediction is given that the example under consideration belongs to class C_k. By examining the fired rule, it can be explained how the prediction is attained. If necessary, the intermediate process can also be explicitly explained.

C4.5 and C4.5rules [Quinlan, 1993] were run on the above three datasets to generate DT rules. Briefly, C4.5 generates a decision tree which C4.5rules generalizes to rules. Since researchers [Cheng et al., 1988; Shavlik et al., 1991] observed that mapping many-valued variables to two-valued variables results in decision trees with higher classification accuracy, the same binary coded data for neural networks were used for C4.5 and C4.5rules.

Being expliable is only one aspect of understandability. A rule with many conditions is harder to understand than a rule with fewer conditions. Too many rules also hinder humans understanding of the data under examination. In addition to understandability, rules without generalization (i.e., high accuracy on testing data) are not much of use. Hence, the comparison is performed along three dimensions: 1. predictive accuracy; 2. average number of conditions of a rule; and 3. number of rules (see Figures 2-4).

The reasoning behind the comparisons is that if NN rules are comparable with DT rules, since the latter are admittedly interpretable, so should the former. Now that each prediction can be explained in light of some rule, and those rules have direct links to the neural network, it can be concluded that the network’s behavior can be understood via those rules.

The comparisons made in Figures 2-4 indicate that NN rules are comparable with, if not better than, DT rules in terms of our understanding measures. The average number of conditions in NN rules is higher than that of DT for 2 of the 3 problems tested, however, the total number of NN rules is less than DT rules for all the 3 problems. These observations are consistent with the nature of each learning algorithm, i.e., parallel vs. sequential. Other issues of interests are:

- The training time. It takes much longer time to train a neural network than to learn a decision tree. This is also true for NN rules and DT rules extraction. Due to the existence of sequential and parallel data types, and decision trees and neural networks are best suited to one type only [Quinlan, 1994], the two approaches are expected to coexist. When time is really scarce, the decision tree approach should be taken. Otherwise, it is worthwhile trying both because of backpropagation’s other advantages (generalizing better on a smaller dataset, predicting better in general, etc. [Towell and Shavlik, 1993]).

- Average performance of NN rules. Because of neural networks’ nondeterministic nature, it is not uncommon that many runs of networks are needed with
• **Accuracy of neural networks and NN rules.** There is a trade-off between the accuracy of the rules extracted from the network and the complexity of the rules. A network can be further pruned and simpler rules obtained at the cost of sacrificing its accuracy. A notable feature of our rule extraction algorithm is that while it allows us to extract rules with the same accuracy level as that of the pruned network, it is also possible to simplify the rules by considering a smaller number of hidden unit activation values.

• **Understanding the weights of connections.** Unlike M-of-N rules [Towell and Shavlik, 1993], NN rules here reflect precisely how the network works. NN rules given here are actually the merge of the two sets: 1. from the input layer to the hidden layer; 2. from the hidden layer to the output layer. NN rules cover all the possible combinations of the connections with various input values and discrete activation values of hidden units. This is a significant improvement over search-based methods [Towell and Shavlik, 1993; Fu, 1994] where all possible input combinations are searched for subsets that will exceed the bias on a unit. To reduce the cost of searching, they normally limit the number of antecedents in extracted rules. Our algorithm imposes no such limit.

• **Consistency between NN and DT rules.** Consistency checking is not an easy task. In general, the possible rule space is very large since the training data is only a sample of the world under consideration. It is not surprising that there exist many equally good rule sets. Using the binary code for the Iris data, for example, the possible size of the rule space is $2^{39}$, but there are only 75 examples for training. However, for simple problem like the Iris problem, the rules extracted by NN and the rules generated by DT are remarkably similar.

5 Conclusion

Neural networks have been considered black boxes. In this paper, we propose to understand a network by rules extracted from it. We describe a three-phase algorithm that can extract rules from a standard feedforward neural network. Network training and pruning is done via the simple and widely-used backpropagation method. No restriction is imposed on the activation values of the hidden units or output units. Extracted rules are a one-to-one mapping of the network. They are compact and comprehensible, and do not involve any weight values. The accuracy of the rules from a pruned network is as high as the accuracy of the network. Experiments show that NN rules and DT rules are quite comparable. Since DT rules are regarded as explicit and understandable, we conclude that NN rules are likewise. With the rules extracted by the method introduced here, neural networks should no longer be regarded as black boxes.

References


