The Shapley Value of Classifiers in Ensemble Games

Benedek Rozemberczki
The University of Edinburgh
Edinburgh, United Kingdom
benedek.rozemberczki@ed.ac.uk

Rik Sarkar
The University of Edinburgh
Edinburgh, United Kingdom
rsarkar@inf.ed.ac.uk

ABSTRACT
What is the value of an individual model in an ensemble of binary classifiers? We answer this question by introducing a class of transferable utility cooperative games called ensemble games. In machine learning ensembles, pre-trained models cooperate to make classification decisions. To quantify the importance of models in these ensemble games, we define Troupe – an efficient algorithm which allocates payoffs based on approximate Shapley values of the classifiers. We argue that the Shapley value of models in these games is an effective decision metric for choosing a high performing subset of models from the ensemble. Our analytical findings prove that our Shapley value estimation scheme is precise and scalable; its performance increases with size of the dataset and ensemble. Empirical results on real world graph classification tasks demonstrate that our algorithm produces high quality estimates of the Shapley value.

ACM Reference Format:
Benedek Rozemberczki and Rik Sarkar. 2018. The Shapley Value of Classifiers in Ensemble Games. In Woodstock ’18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY.
ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION
The advent of black box machine learning models raised fundamental questions about how input features and individual training data points contribute to the decisions of expert systems [17, 28]. There has also been interest in how the heterogeneity of models in an ensemble results in heterogeneous contributions of those to the classification decisions of the ensemble [16, 47]. For example one would assume that computer vision, credit scoring and fraud detection systems which were trained on varying quality proprietary datasets output labels for data points with varying accuracy. Another source of varying model performance can be the complexity of models e.g. the number of weights in a neural network or the depth of a classification tree.

Quantifying the contributions of models to an ensemble is paramount for practical reasons. Given the model valuations, the gains of the task can be attributed to specific models, large ensembles can be reduced to smaller ones without losing accuracy [22, 32] and performance heterogeneity of ensembles can be gauged [16]. This raises the natural question: How can we measure the contributions of models to the decisions of the ensemble in an efficient, model type agnostic, axiomatic and data driven manner?

We frame this question as one of valuation of models in an ensemble. The solution to the problem requires an analytical framework to assess the worth of individual classifiers in the ensemble. This idea is described in Figure 1. Each classifier in the ensemble receives the data points, and they output for each data point a probability distribution over the potential classes. An oracle – which has access to the ground truth – quantifies the worth of models in the ensemble. These importance metrics can be used to make decisions – e.g. pruning the ensemble and allocation of payoffs.

Present work. We introduce ensemble games, a class of transferable utility cooperative games [35]. In these games binary classifiers which form an ensemble play a voting game to assign a binary label to a data point by utilizing the features of the data point. Building on the ensemble games we derive dual ensemble games in which the classifiers cooperate in order to misclassify a data point. We do this to characterize the role of models in incorrect decisions.
We argue that the Shapley value [41], a solution concept from cooperative game theory, is a model importance metric. The Shapley value of a classifier in the ensemble game defined for a data point can be interpreted as the probability of the model becoming the pivotal voter in a uniformly sampled random permutation of classifiers. Computing the exact Shapley values in an ensemble game would take factorial time in the number of classifiers. In order to alleviate this we exploit an accurate approximation algorithm of the individual Shapley values which was tailored to voting games [12]. We propose Troupe, an algorithm which approximates the average of Shapley values in ensemble games and dual games using data. We utilize the average Shapley values as measures of model importance in the ensemble and discuss that the Shapley values are interpretable as an importance distribution over classifiers.

We evaluate Troupe by performing various classification tasks. Using data from real world webgraphs (Reddit, GitHub, Twitch) we demonstrate that Troupe outputs high quality estimates of the Shapley value. We validate that the Shapley value estimates of Troupe can be used as a decision metric to build space efficient and accurate ensembles. Our results establish that more complex models in an ensemble have a prime role in both correct and incorrect decisions.

**Main contributions.** Specifically the contributions of our work can be summarized as:

1. We propose ensemble games and their dual games to model the contribution of individual classifiers to the decisions of voting based ensembles.
2. We design Troupe an approximate Shapley value based algorithm to quantify the role of classifiers in decisions.
3. We provide a probabilistic bound for the approximation error of average Shapley values estimated from labeled data.
4. We empirically evaluate Troupe for model valuation and forward ensemble building on graph classification tasks.

The rest of this work has the following structure. In Section 2 we discuss related work on the Shapley value, its approximations and applications in machine learning. We introduce the concept of ensemble games in Section 3 and discuss Shapley value based model valuation in Section 4 with theoretical results. We evaluate the proposed algorithm experimentally in Section 5. We summarize our findings in Section 6 and discuss future work. The reference implementation of Troupe is available at https://github.com/username/repositoryname [Anonymized for double blind review].

## 2 RELATED WORK

Our model pruning framework intersects with research about the Shapley value and existing approaches to ensemble pruning.

### 2.1 The Shapley value

The Shapley value [41] is a solution to the problem of distributing the gains among players in a transferable utility cooperative game [35]. It is widely known for its desirable axiomatic properties [6] such as efficiency and linearity. However, exact computation of Shapley value takes factorial time, making it intractable in games with a large number of players. General [29, 37] and game specific [12] approximation techniques have been proposed. In Table 1, we compare various approximation schemes with respect to certain desired properties.

Shapley values can be approximated using a Monte Carlo MLE sampling of the permutations of players and also with a truncated Monte Carlo sampling variant TMC [29, 30, 53]. A more tractable approximation is proposed in [37], using a multilinear extension (MLE) of the Shapley value. A variant of this technique [23, 24] calculates the value of large players explicitly and applies the MLE technique to small ones. The only approximation technique tailored to weighted voting games is the expected marginal contributions method (EMC) which estimates the Shapley values based on contributions to varying size coalitions. Our proposed algorithm Troupe builds on EMC.

| Method   | Voting Bound Non-Random Space Time |
|----------|-----------------------------------|
| Explicit | ✔ ✔ ✔ O(m) O(m^2)                 |
| MC [30]  | ✘ ✔ ✔ O(m) O(m^3)                 |
| TMC [17] | ✘ ✔ ✔ O(m) O(mp)                  |
| MLE [37] | ✘ ✘ ✔ O(m) O(m)                   |
| MMLE [23, 24] | ✘ ✘ ✔ O(m) O(m) |
| EMC [12] | ✔ ✔ ✔ O(m) O(m^2) |

Shapley value has previously been used in machine learning for measuring feature importance [8, 13, 21, 26, 27, 33, 38]. In the feature selection setting the features are seen as players that cooperate to achieve high goodness of fit. Various discussed approximation schemes [9, 29, 43] have been exploited to make feature importance quantification in high dimensional spaces feasible [10, 28, 44, 45, 50] when explicit computation is not tractable. Another machine learning domain for applying the Shapley value was the pruning of neural networks [1, 18, 42]. In this context approximate Shapley values of hidden layer neurons are used to downsize overparametrized classifiers. It is argued in [42] that pruning neurons is analogous to feature selection on hidden layer features. Finally, there has been increasing interest in the equitable valuation of data points with game theoretic tools [17, 20]. In such settings the estimated Shapley values are used to gauge the influence of individual points on a supervised model. These approximate scores are obtained with group testing of features [20] and permutation sampling [5, 17].

### 2.2 Ensemble pruning and building

We compare Troupe to existing ensemble pruning and building approaches in terms of desired properties in Table 2. As one can see our framework is the only one which has all of these characteristics. Specifically, these properties are:

- **Agnostic:** The procedure can prune/build ensembles of heterogeneous model types, not just a specific type (e.g. trees).
- **Set based:** An algorithm is able to return a subset of models with a high-performance, not just a single one.
- **Diverse:** The value of individual models is implicitly or explicitly affected by how diverse their predictions are.
• **Bidirectional**: A bidirectional ensemble selection technique can select a sub-ensemble in a forward or backward manner.

**Table 2**: Comparison of ensemble pruning and building techniques in terms of having (✔) and missing (✘) desirable data.

| Method          | Agnostic | Set based | Diverse | Bidirectional |
|-----------------|----------|-----------|---------|---------------|
| Greedy [4]      | ✔        | ✔         | ✘       | ✔             |
| WV-LP [51]      | ✔        | ✔         | ✘       | ✘             |
| RE [31]         | ✔        | ✔         | ✘       | ✘             |
| DREP [25]       | ✔        | ✔         | ✔       | ✘             |
| COMEP [2]       | ✔        | ✔         | ✔       | ✘             |
| EP-SDP [52]     | ✔        | ✔         | ✘       | ✘             |
| Troupe (ours)   | ✘        | ✘         | ✔       | ✘             |

3 ENSEMBLES GAMES

We now introduce a novel class of co-operative games and examine axiomatic properties of solution concepts which can be applied to these games. We will discuss shapley value as an exact solution for these games, [41], and discuss approximations of the Shapley value based solution [12, 30, 37].

3.1 Ensemble game

We define an ensemble game to be one where binary classifier models (players) co-operate to label a single data point. The aggregated decision of the ensemble is assumed to be made by a vote of the players. We assume that a set of labelled data points are known:

**Definition 1. Labeled data point.** Let \((x, y)\) be a labeled data point where \(x \in \mathbb{R}^d\) is the feature vector and \(y \in \{0, 1\}\) is the corresponding binary label.

Our work considers arbitrary binary classifier models (e.g., classification trees, support vector machines, neural networks) that operate on the same input feature vector \(x\). This approach is agnostic of the exact type of the model, we only assume that \(M\) can output a probability of the data point having a positive label. The model owner does not access the label, just a probability of \(y = 1\) is output by the model.

**Definition 2. Positive classification probability for model M.** Let \((x, y)\) be a labeled data point and \(M\) be a binary classifier, \(P(y = 1 \mid M, x)\) is the probability of the data point having a positive label output by classifier \(M\).

We are now ready to define the operation of an ensemble classifier consisting of multiple models.

**Definition 3. Ensemble.** An ensemble is a set \(M\) of size \(m\) that consists of binary classifier models \(M \in M\) which can each output a probability for a data point \(x \in \mathbb{R}^d\) having a positive label. The ensemble sets the probability of a label as:

\[
P(y = 1 \mid M, x) = \sum_{M \in M} P(y = 1 \mid M, x)/m.
\]

And it makes decision about the label as:

\[
\hat{y} = \begin{cases} 
1 & \text{if } P(y = 1 \mid M, x) \geq \gamma, \\
0 & \text{otherwise}.
\end{cases}
\]

where \(0 \leq \gamma \leq 1\) is the decision threshold and \(\hat{y}\) is the predicted label of the data point.

**Definition 4. Sub-ensemble.** A sub-ensemble \(S\) is a subset \(S \subseteq M\) of binary classifier models.

**Definition 5. Individual model weight.** The individual weight of the vote for \(M\), in sub-ensemble \(S \subseteq M\) for data point \((y, x)\) is defined as:

\[
w_M = \begin{cases} 
P(y = 1 \mid M, x)/m & \text{if } y = 1, \\
P(y = 0 \mid M, x)/m & \text{otherwise}.
\end{cases}
\]

Under this definition, the individual model weight of any binary classifier \(M \in M\) is bounded: \(0 \leq w_M \leq 1/m\). Note that the weight of \(M \in S\) depends on \(m\) – the size of the larger ensemble and not on the size \(|S|\) of the sub-ensemble.

**Definition 6. Ensemble game.** Let \(M\) be a set of binary classifiers. An ensemble game for a labeled data point \((y, x)\) is then a co-operative game \(G = (M, v)\) in which:

\[
v(S) = \begin{cases} 
1 & \text{if } w(S) \geq \gamma, \\
0 & \text{otherwise}.
\end{cases}
\]

where \(w(S) = \sum_{M \in S} w_M\) for any sub-ensemble \(S \subseteq M\) and threshold \(0 \leq \gamma \leq 1\).

This definition is the central idea in our work. The models in the ensemble play a cooperative voting game to classify the data point correctly. When the data point is classified correctly the payoff is 1, an incorrect classification results in a payoff of 0. Each model casts a weighted vote about the data point and our goal is going to be to quantify the value of individual models in the final decision. In other words, we would like to measure how individual binary classifiers contribute on average to the correct classification of a specific data point. This solution concept is described in the next section (3.2).

We can consider a misclassification as a dual ensemble game:

**Definition 7. Dual ensemble game.** Let \(M\) be a set of binary classifiers. A dual ensemble game for a labeled data point \((y, x)\) is then a co-operative game \(G = (M, \bar{v})\) in which:

\[
\bar{v}(S) = \begin{cases} 
1 & \text{if } \bar{w}(S) \geq \bar{\gamma}, \\
0 & \text{otherwise}.
\end{cases}
\]

for a binary classifier ensemble vote score \(0 \leq \bar{w}(S) \leq 1\) where \(\bar{w}(S) = \sum_{M \in S} (1/m - w_M)\) for any sub-ensemble \(S \subseteq M\) and inverse cutoff value \(0 \leq \bar{\gamma} \leq 1\) defined by \(\bar{\gamma} = 1 - \gamma\).

If the sum of classification weights for the binary classifiers is below the cutoff value the models in the ensemble misclassify the point, lose the ensemble game and as a consequence receive a payoff that is zero. In such scenarios it is interesting to ask: how can we describe the role of models in the misclassification? The dual ensemble game is derived from the original ensemble game in order to characterize this situation.

The classification game and its dual can be reframed simply as:

**Definition 8. Simplified ensemble game.** An ensemble game in simplified form is described by the cutoff value weight-vector tuple \(\gamma, \{w_1, \ldots, w_m\}\).
We have defined the binary classification problem with an ensemble which always has a zero marginal contribution in any sub-ensemble on the dataset. This property will imply that valuations of a binary classifier ensemble. Now we will argue that as a weighted voting game, which is a type of co-operative game.

3.2 Solution concepts for model valuation

We have defined the binary classification problem with an ensemble as a weighted voting game, which is a type of co-operative game. Now we will argue that solution concepts of co-operative games are suitable for the valuation of individual models which form the binary classifier ensemble.

**Definition 10. Solution concept.** A solution concept defined for the ensemble game \( G = (M, v) \) is a function which assigns the real value \( \Phi(M, v) \in \mathbb{R} \) to each binary classifier \( M \in M \).

The scalar \( \Phi(M) \) can be interpreted as the value of the individual binary classifier \( M \) in the ensemble \( M \). In the following we discuss axiomatic properties of solution concepts which are the desiderata for model valuation functions, and the implications of the axioms in the context of model valuation in binary ensemble games.

**Axiom 1. Null classifier.** A solution concept has the null classifier property if \( \forall S \subseteq M : v(S \cup \{M\}) = v(S) \) then \( \Phi(M, v) = 0 \).

Having the null classifier property means that a binary classifier which always has a zero marginal contribution in any sub-ensemble will have a zero payoff on its own. This also implies that the classifier never casts the deciding vote to correctly classify the data point when it is added to a sub-ensemble. Conversely, in the dual ensemble game the model never contributes to the misclassification of the data point.

**Axiom 2. Efficiency.** A solution concept satisfies the efficiency property if \( v(M) = \sum_{M \in M} \Phi(M, v) \).

That is, the value (loss or gain) of an ensemble can be split precisely into the contributed value of the constituent models.

**Axiom 3. Symmetry.** A solution concept has the symmetry property if \( \forall S \subseteq M \setminus \{M', M''\} : v(S \cup \{M\}) = v(S \cup \{M''\}) \) implies that \( \Phi(M', v) = \Phi(M'', v) \).

Two binary classifiers which make equal marginal contribution to all sub-ensembles have the same value in the full ensemble.

**Axiom 4. Linearity.** A solution concept has the linearity property if given any two ensemble games \( G = (M, v) \) and \( G' = (M, v') \) on the same set \( M \), the binary classifier \( M \) satisfies \( \Phi(M, v + v') = \Phi(M, v) + \Phi(M, v') \).

That is, the value in the combined game is the sum of the values in individual games. This property will imply that valuations of a model for different datapoints, when added, leads to its valuation on the dataset.

### 3.3 The Shapley value

The Shapley value [41] of a classifier is the average marginal contribution of the model over the possible different permutations in which the ensemble can be formed [6]. It is a solution concept which satisfies Axioms 1-4 and is the only solution concept which is uniquely characterized by Axioms 3 and 4.

**Definition 11. Shapley value.** The Shapley value of binary classifier \( M \) in the ensemble \( M \), for the data point level ensemble game \( G = (M, v) \) is defined as

\[
\Phi_M(v) = \sum_{S \subseteq M \setminus \{M\}} \frac{|S|! |M| - |S| - 1|!}{|M|!} (v(S \cup \{M\}) - v(S)).
\]

Calculating the exact Shapley value for every model in an ensemble game would take \( O(m!) \) time, or more, which is computationally unfeasible in large ensembles. We discuss a range of approximation approaches in detail which can give Shapley value estimates in \( O(m) \) and \( O(m^2) \) time.

#### 3.3.1 Multilinear extension (MLE) approximation of the Shapley value

The MLE approximation of the Shapley value in a voting game [12, 37] can be used to estimate the Shapley value in the ensemble game and its dual game. Let us define the expectation and the variation of the aggregated ensemble contributions for the remaining models as: \( \mu_M = \sum_{j=1}^{m} w_j - w_M \) and \( \nu_M = \sum_{j=1}^{m} w_j^2 - w_M^2 \). For a classifier \( M \in M \) the multi-linear approximation of the unnormalized Shapley value is computed by:

\[
\tilde{\Phi}_M = \frac{1}{\sqrt{2\pi\mu_M}} \exp \left(-\frac{(x - \mu_M)^2}{2\nu_M}\right) dx - \frac{1}{\sqrt{2\pi\mu_M}} \exp \left(-\frac{(x - \mu_M)^2}{2\nu_M}\right) dx.
\]

This approximation assumes that the size of the game is large (many classifiers in the ensemble in our case) and also that \( \mu \) has an approximate normal distribution. Calculating all of the approximate Shapley values by MLE takes \( O(m) \) time.

#### 3.3.2 Monte Carlo (MC) approximation of the Shapley value

The MC approximation [29, 30] given the ensemble \( M \) estimates the Shapley value of the model \( M \in M \) by the average marginal contribution over uniformly sampled permutations.

\[
\Phi_M = \mathbb{E}_{\theta \sim \Theta} [v(S^M \cup \{M\}) - v(S^M \cup \{M\})].
\]

In Equation (1), \( \Theta \) is a uniform distribution over the \( m! \) permutations of the binary classifiers and \( S^M \) is the subset of models that appear before the classifier \( M \) in permutation \( \theta \). Approximating the Shapley value requires the generation of \( p \) classifier permutations (for a suitable \( p \)), and marginal contribution calculations with respect to those contributions – this takes \( O(mp) \) time.

#### 3.3.3 Voting game approximation of the Shapley value

The ensemble games introduced above are a variant of voting games [36], hence we can use the Expected Marginal Contributions (EMC) approximation [12]. This procedure sums the expected marginal contributions of a model to fixed size ensembles – it is described in the pseudo-code Algorithm 1.

The algorithm iterates over the individual model weights and initializes Shapley values as zeros (lines 1-2). For each ensemble size it calculates the expected contribution of the model to the ensemble.
This expected contribution is the probability that a classifier becomes the marginal voter. These marginal contributions are added to the approximate Shapley value (lines 3-8). Using this Shapley value approximation technique takes $O(m^2)$ time. However, it is the most accurate Shapley value approximation technique in terms of absolute error of the Shapley value estimates [12].

\begin{algorithm}
\caption{Expected marginal contribution approximation of Shapley values based on [12].}
\begin{algorithmic}[1]
\State \textbf{Data:} $[w_1,\ldots,w_m]$ – Weights of binary classifiers.
\State \hspace{0.5cm} $\gamma$ – Cutoff value.
\State \hspace{0.5cm} $\delta$ – Numerical stability parameter.
\State \hspace{0.5cm} $\mu$ – Expected value of weights.
\State \hspace{0.5cm} $v$ – Variance of weights.
\State \hspace{0.5cm} \textbf{Result:} $(\hat{\varphi}_1,\ldots,\hat{\varphi}_m)$ – Approximate Shapley values.
\For{$j \in \{1,\ldots,m\}$}
\State $\hat{\varphi}_j \gets 0$
\For{$k \in \{1,\ldots,m-1\}$}
\State $a \gets (\gamma - w_j) / k$
\State $b \gets (\gamma - \delta) / k$
\State $\hat{\varphi}_j \leftarrow \frac{1}{\sqrt{2\pi v^2}} \int_a^b \exp(-k \frac{(x-a)^2}{2v^2}) dx$
\EndFor
\EndFor
\end{algorithmic}
\end{algorithm}

\begin{algorithm}
\caption{Calculating the individual model weights in an ensemble game given a data point and a classifier ensemble.}
\begin{algorithmic}[1]
\State \textbf{Data:} $(x,y)$ – Labeled data point.
\State $\{M_1,\ldots,M_m\}$ – Set of binary classifiers.
\State \textbf{Result:} $[w_1,\ldots,w_m]$ – Weights of individual models.
\For{$j \in \{1,\ldots,m\}$}
\If{$y = 1$}
\State $w_j \leftarrow P(y = 1 \mid M_j, x) / m$
\Else
\State $w_j \leftarrow P(y = 0 \mid M_j, x) / m$
\EndIf
\EndFor
\end{algorithmic}
\end{algorithm}

Figure 2: The approximate average Shapley value calculation pipeline. (a) Given the set of labeled datapoints the data owner sends the features of data points to the binary classifiers in the ensemble. (b) The models in the ensemble score each of the data points independently and send the probability scores back to the oracle. (c) Given the label and the scores the oracle defines the ensemble game on each of the data points. (d-e) The ensemble games and the dual ensemble games are solved by the oracle and approximate Shapley values of models are calculated in each of the data point level ensemble games.

4 MODEL VALUATION WITH THE SHAPLEY VALUE OF ENSEMBLE GAMES

In this section we present Troupe, the mechanism used for model valuation in ensembles. The chart in Figure 2 gives a high-level summary of our model valuation approach.

4.1 The model valuation algorithm

The Shapley value-based model evaluation procedure described by Algorithm 3 uses $D = \{(x_1, y_1) ; \ldots ; (x_n, y_n)\}$, a set of $n$ datapoints with binary labels, for evaluating the ensemble $M$ given a cutoff value $0 \leq \gamma \leq 1$ and a numerical stability parameter $\delta \in \mathbb{R}^{+}$. We set $m$ the number of models and $n$ the number of labeled data points used in the model valuation (lines 1-2). We iterate over all of the data points (line 3) and given a data point for all of the models we compute the individual model weights in an ensemble game using the label, features and the model itself (line 4) – see Algorithm 2 for the exact details. Using the individual model weights in the ensemble game we calculate the expected value and variance of the data point (lines 5-6).

If the sum of individual model weights is higher than the cutoff value (line 7) the Shapley values in the ensemble game are approximated by Algorithm 1 for the data point (line 8). The Shapley values in the dual ensemble game are defined by a vector of zeros (line 9). If the point is misclassified (line 10) a dual ensemble game is defined for the data point. This requires the redefined cutoff value $\hat{\gamma}$, expected value $\hat{\mu}$ and variance $\hat{\nu}$ of the individual model weight vector (lines 11-13). We exploit the linearity of expectation and the location invariance of the variance. The individual model weight vector is redefined (line 14) in order to quantify the role of models in the erroneous decision. The original ensemble game Shapley values are initialized with zeros (line 15) and using the new parametrization of the game we approximate the dual ensemble game Shapley values (line 16) by Algorithm 1. The algorithm outputs data point level Shapley values for each model.
Data: \( \mathcal{D} \) – Labeled data points. 
\( M \) – Set of binary classifiers. 
\( \gamma \) – Cutoff value. 
\( \delta \) – Numerical stability parameter.

Result: 
\( \{ \tilde{\Phi}^+_{m}, \ldots, \tilde{\Phi}_{m}^+ \}, \ldots, \{ \tilde{\Phi}^+_{n}, \ldots, \tilde{\Phi}_{m}^+ \} \)

Shapley value vectors for ensemble games.
\( \{ \tilde{\Phi}^-_{m}, \ldots, \tilde{\Phi}_{m}^- \}, \ldots, \{ \tilde{\Phi}^-_{n}, \ldots, \tilde{\Phi}_{m}^- \} \)

Shapley value vectors for dual ensemble games.

### 4.2 Measuring ensemble heterogeneity

The data point level Shapley values of ensemble games and their dual can be aggregated to measure the importance of models in ensemble level decisions.

In order to quantify the role of models in classification and misclassification we calculate the average Shapley value of models in the ensemble and dual ensemble games conditional on the success of classification. The sets \( N^+ \) and \( N^- \) contain the indices of classified and misclassified data points. Using the cardinality of these sets \( n^+ = |N^+|, n^- = |N^-| \) and the data point level Shapley values output by Algorithm 1 we can estimate the conditional role of models in classification and misclassification by averaging the approximate Shapley values using Equations (2) and (3).

\[
\begin{align*}
(\tilde{\Phi}^+_{1}, \ldots, \tilde{\Phi}^+_{m}) &= \sum_{i \in N^+} (\tilde{\Phi}^+_{0}, \ldots, \tilde{\Phi}^+_{m})/n^+ & (2) \\
(\tilde{\Phi}^-_{1}, \ldots, \tilde{\Phi}^-_{m}) &= \sum_{i \in N^-} (\tilde{\Phi}^-_{0}, \ldots, \tilde{\Phi}^-_{m})/n^- & (3)
\end{align*}
\]

If a component of the average Shapley value vector in Equation (2) is large compared to other components the corresponding model has an important role in the correct classification decisions of the ensemble. A large component in Equation (3) corresponds to a model which is responsible for a large number of misclassifications.

### 4.3 Theoretical properties

Our framework utilizes labeled data instances to approximate the importance of classifiers in the ensemble and this has important implications. In the following we discuss how the size of the dataset and the number classifiers affects the Shapley value approximation error and the runtime of Troupe.

#### 4.3.1 Bounding the average approximation error.

Our discussion focuses on the average conditional Shapley value in ensemble games. However, analogous results can be obtained for the Shapley values computed from dual ensemble games.

**Definition 12. Approximation error.** The Shapley value approximation error of model \( M \in \mathcal{M} \) in an ensemble game is defined as \( \Delta\Phi_M = \bar{\Phi}_M - \Phi_M^* \).

**Definition 13. Average approximation error.** Let us denote the Shapley value approximation errors of model \( M \in \mathcal{M} \) calculated from the dataset \( \mathcal{D} \) of correctly classified points as \( \Delta\Phi^+_M \), \ldots, \( \Delta\Phi^+_M \). The average approximation error is defined by \( \hat{\Delta}\Phi_M = \sum_{i=1}^n \Delta\Phi^+_M/n \).

**Theorem 1. Average conditional Shapley value approximation error bound.** If the Shapley value approximation errors \( \Delta\Phi^+_M, \ldots, \Delta\Phi^+_M \) of model \( M \in \mathcal{M} \) calculated by Algorithm 3 from the dataset \( \mathcal{D} \) are independent random variables then for any \( \varepsilon \in \mathbb{R}^+ \) Inequality (4) holds.

\[
P(\hat{\Delta}\Phi_M - \mathbb{E}[\hat{\Delta}\Phi_M^*] \geq \varepsilon) \leq 2 \exp\left( -\frac{\varepsilon^2}{8m} - \frac{n^2 \cdot m \cdot \varepsilon^4}{8} \right) \]  

**Proof.** Let us first note the fact that every absolute Shapley approximation value is bounded by the inequality described in Lemma 1.

**Lemma 1. Approximate Shapley value bound.** As Theorem (10) of [12] states the approximation error of the Shapley value in a single voting game is bounded by Inequality (5) when the expected marginal contributions approximation is used.

\[
-\sqrt{\frac{8}{m\pi}} \leq \Delta\Phi^*_M \leq \sqrt{\frac{8}{m\pi}}
\]  

Using Lemma 1, the fact that Troupe is based on the expected marginal contributions approximation and that the Shapley values of a model in different ensemble games are independent random variables we can use Hoeffding’s second inequality [19] for bounded non zero-mean random variables:

\[
P(\Delta\Phi^*_M - \mathbb{E}[\Delta\Phi^*_M] \geq \varepsilon) \leq 2 \exp\left( -\frac{\varepsilon^2}{8m} \right)
\]

\[
P(\Delta\Phi^*_M - \mathbb{E}[\Delta\Phi^*_M] \geq \varepsilon) \leq 2 \exp\left( \frac{2\varepsilon^2}{2n} \right)
\]  

\[\Box\]
Theorem 2. Confidence interval of the expected average approximation error. In order to acquire an \((1 - \alpha)\)-confidence interval of \(\mathbb{E}[\Delta \Phi_M] \pm \varepsilon\) one needs a labeled dataset \(\mathcal{D}\) of correctly classified data points for which \(n\) the cardinality of \(\mathcal{D}\), satisfies Inequality (6).

\[
n \geq \frac{8 \ln^2 \left( \frac{2}{\alpha} \right)}{\varepsilon^4 mn^2}
\]

Proof. The probability \(P(\|\Delta \Phi_M - \mathbb{E}[\Delta \Phi_M]\| \geq \varepsilon)\) in Theorem 1 equals to the level of significance for the confidence interval \(\mathbb{E}[\Delta \Phi_M] \pm \varepsilon\). Which means that Inequality (7) holds for the significance level \(\alpha\).

\[
\alpha \leq 2 \exp \left( -\sqrt{\frac{n^2 \cdot m \cdot \varepsilon^2}{8}} \right).
\]

Solving inequality (7) for \(n\) yields the cardinality of the dataset (number of correctly classified data points) required for obtaining the confidence interval described in Theorem 2. □

The inequality presented in Theorem 2 has two important consequences regarding the bound:

1. Larger ensembles require less data in order to give confident estimates of the Shapley value for individual models.
2. The dataset size requirement is sublinear in terms of confidence level and quadratic in the precision of the Shapley value approximation.

4.3.2 Runtime and memory complexity. The runtime and memory complexity of the proposed model valuation framework depends on the complexity of the main evaluation phases. We assume that our framework operates in a single-core non distributed setting.

**Scoring and game definition.** Assuming that the scoring of a data point takes \(O(1)\) time, scoring the data point with all models takes \(O(m)\). Scoring the whole dataset and defining games both takes \(O(nm)\) time and \(O(nm)\) space respectively.

**Approximation and overall complexity.** Calculating the expected marginal contribution of a model to a fixed size ensemble takes \(O(1)\) time. Doing this for all of the ensemble sizes takes \(O(m)\) time. Approximating the Shapley value for all models requires \(O(m^2)\) time and \(O(m)\) space. Given a dataset of \(n\) points this implies a need for \(O(nm^2)\) time and \(O(nm)\) space. This is also the overall time and space complexity of the proposed framework.

5 EXPERIMENTAL EVALUATION

In this section, we show that Troupe approximates the average of Shapley values precisely. We provide evidence that Shapley values are a useful decision metric for ensemble creation. Our results illustrate that model importance and complexity are correlated, and that Shapley values are able to identify adversarial models in the ensemble. Our evaluation is based on various real world binary graph classification tasks [39]. Specifically, we use datasets collected from Reddit, Twitch and GitHub – the descriptive statistics of these datasets are in Table 3.

| Dataset | Classes | Nodes | Density | Diameter |
|---------|---------|-------|---------|----------|
| Reddit  | 522     | 479   | 11      | 93       |
| Twitch  | 520     | 480   | 14      | 52       |
| GitHub  | 552     | 448   | 10      | 942      |

Table 3: Descriptive statistics of the graph classification datasets taken from [39] used for the evaluation of Troupe.

5.1 The precision of approximation

The Shapley value approximation performance of Troupe is compared to that of various other estimation schemes [29, 37] discussed earlier. We use an ensemble of logistic regressions where each classifier is trained on features extracted with a whole graph embedding technique [40, 46, 48]. We utilize 50% of the graphs for training and calculated the average conditional Shapley values of ensemble games and dual ensemble games using the remaining 50% of the data.

5.1.1 Experimental details. The features of the graphs are extracted with whole graph embedding techniques implemented in the open source Karate Club framework [39]. Given a set of graphs \(G = (G_1, \ldots, G_n)\) whole graph embedding algorithms [40, 46] learn a mapping \(g : G \rightarrow \mathbb{R}^d\) which delineate the graphs \(G \in G\) to a \(d\) dimensional metric space. We utilize the following whole graph embedding and statistical fingerprinting techniques:

1. **FEATHER** [40] uses the characteristic function of topological features as a graph level statistical descriptor.
2. **Graph2Vec** [34] extracts tree features from the graph.
3. **GL2Vec** [7] distills tree features from the dual graph.
4. **NetLSD** [46] derives characteristics of graphs using the heat trace of the graph spectra.
5. **SF** [11] utilizes the largest eigenvalues of the graph Laplacian matrix as an embedding.
6. **LDP** [3] sketches the histogram of local degree distributions.
7. **GeoScattering** [15] applies the scattering transform to various structural features (e.g. degree centrality).
8. **IGE** [14] combines graph features from local degree distributions and scattering transforms.
9. **FGSD** [48] sketches the Moore-Penrose spectrum of the normalized graph Laplacian with a histogram.

The embedding techniques use the default settings of the Karate Club library, each embedding dimension is column normalized and the graph features are fed to the scikit-learn implementation of logistic regression. This classifier is trained with \(\ell_2\) penalty cost, we choose an SGD optimizer and the regularization coefficient \(\lambda\) was set to be \(10^{-3}\).

5.1.2 Experimental findings. In Table 4 we summarize the absolute percentage error values (compared to exact Shapley values in ensemble games) obtained with the various approximations schemes. (i) Our empirical results support that Troupe consistently computes accurate estimates of the ground truth model evaluations across datasets and classifiers in the ensemble. (ii) The high quality of estimates suggests that the approximate Shapley values of models extracted by Troupe can serve as a proxy decision metric for ensemble building and model selection.
Table 4: Absolute percentage error of average conditional Shapley values obtained by approximation techniques (rows) for the graph classifiers (columns) in the ensemble game. Bold numbers note the lowest error on each dataset – classifier pair.

| Approximation | FEATHER | Graph2Vec | GL2Vec | NetLSD | SF | LDP | GeoScatter | IGE | FGSD |
|---------------|---------|-----------|--------|--------|----|-----|------------|-----|------|
| **Reddit**    |         |           |        |        |    |     |            |     |      |
| Troupe        | 1.23    | 2.35      | 8.18   | 0.99   | 2.64 | 2.31 | 1.64       | 4.85 | 1.49 |
| MLE           | 3.20    | 23.61     | 32.62  | 4.19   | 5.34 | 7.97 | 7.12       | 5.42 | 7.61 |
| MC $p = 10^3$ | 12.57   | 30.94     | 13.26  | 8.67   | 32.76| 12.32| 11.62      | 16.36| 12.78|
| MC $p = 10^3$ | 4.71    | 5.38      | 3.41   | 1.67   | 3.03 | 5.51 | 4.34       | 4.97 | 3.82 |
| **Twitch**    |         |           |        |        |    |     |            |     |      |
| Troupe        | 0.28    | 3.33      | 1.18   | 2.53   | 1.62 | 0.59 | 1.48       | 0.25 | 1.19 |
| MLE           | 5.22    | 5.44      | 3.05   | 8.32   | 2.38 | 1.92 | 3.14       | 4.85 | 5.77 |
| MC $p = 10^2$ | 2.37    | 10.40     | 6.76   | 7.07   | 15.79| 6.36 | 13.99      | 23.96| 0.39 |
| MC $p = 10^3$ | 2.32    | 4.60      | 2.96   | 2.67   | 2.53 | 2.73 | 6.31       | 0.27 | 3.89 |
| **GitHub**    |         |           |        |        |    |     |            |     |      |
| Troupe        | 2.68    | 0.18      | 2.61   | 1.41   | 1.49 | 1.23 | 1.88       | 2.36 | 1.04 |
| MLE           | 9.22    | 5.12      | 3.76   | 3.27   | 9.71 | 7.46 | 5.08       | 4.04 | 0.73 |
| MC $p = 10^2$ | 5.91    | 9.37      | 4.67   | 9.82   | 8.78 | 8.34 | 13.66      | 28.95| 0.76 |
| MC $p = 10^3$ | 3.35    | 6.09      | 7.70   | 3.26   | 2.84 | 0.79 | 6.67       | 2.51 | 1.12 |

5.2 Ensemble building

Our earlier results suggested that the approximate Shapley values output by Troupe (and other estimation methods) can be used as decision metrics for ensemble building.

5.2.1 Experimental settings. We demonstrate this by selecting a high performance subset of a random forest in a forward fashion using the estimated model valuation scores. From each graph we extract Weisfeiler-Lehman tree features [34] and keep those topological patterns which appeared in at least 5 graphs. Utilizing the counts of these features in graphs we define statistical descriptors. The selection procedure and evaluation steps are the following:

1. Using 40% of the graphs we train a random forest with 50 classification trees, each tree is trained on 20 randomly sampled Weisfeiler-Lehman features – we use the default settings of scikit-learn.
2. We calculate the average conditional Shapley value of classifiers in the games using 30% of the data.
3. We order the classifiers by the approximate Shapley values in decreasing order, create subensembles in a forward fashion and calculate the predictive performance of the resulting subensembles on the remaining 30% of the graphs.

The test performance (measured by AUC scores) of these classifiers and baselines as a function of ensemble size is plotted on Figure 3.

5.2.2 Experimental findings. Our results suggest that Troupe has a material advantage over competing Shapley value approximation schemes. Moreover, the proposed method outperforms the selection of ensemble building baselines on the Twitch and Reddit datasets [25, 31, 51, 52]. This implies that Troupe is a good alternative for existing ensemble pruning techniques and our choice of the Shapley value approximation scheme is justified in practical applications.

Figure 3: The classification performance of ensembles as a function of ensemble size selected by our forward model building procedure and baselines.

5.3 Model complexity and influence

The Shapley value gives an implicit measure of model influence on the ensemble. It is interesting to see whether there is a connection between relative importance and model complexity (e.g. depth of trees or number of neurons). In order to investigate this, we create a voting expert which consists of neural networks with heterogeneous model complexity.

Figure 4: The distribution of normalized Shapley values for neural networks in ensemble and dual ensemble games conditional on the number of neurons.
5.3.1 Experimental settings. We create an ensemble of $m = 10^3$ neural networks using scikit-learn – each of these has a single hidden layer. Each model receives 20 randomly selected frequency features as input and has a randomly chosen number of hidden layer neurons – we uniformly sample this hyperparameter from $\{2^3, 2^4, 2^5, 2^6, 2^7\}$. Individual neural networks are trained by minimizing the binary cross-entropy with SGD for 200 epochs with a learning rate of $10^{-2}$.

5.3.2 Experimental findings. The distribution of normalized average Shapley values for the Reddit dataset are plotted on Figure 4 for the ensemble and dual ensemble games conditioned on the number of hidden layer neurons. The results imply that more complex models with a larger number of free parameters receive higher Shapley values in both classes of games. In simple terms complex models contribute to correct and incorrect classification decisions at a disproportionate rate.

5.4 Identifying adversarial models

Ensembles can be formed by the model owners submitting their classifiers voluntarily to a machine learning market. We investigated how adversarial behaviour of model owners affects the Shapley values of classifiers.

![Figure 5: The mean Shapley value (standard errors added) of adversarial and base classifiers in ensemble games as a function of adversarial noise ratio mixed to predictions.](image)

5.4.1 Experimental settings. We use the Weisfeiler-Lehman tree features described in Subsections 5.2 and 5.3 to train a random forest ensemble of 20 classifiers using 50% of the data – each of these models utilizes a random subset of 20 features and had a maximal tree depth of 4. The Shapley values are calculated from the remaining 50% of the data using Troupe. We artificially corrupt the predictions for 10 of the classification trees by mixing the outputted probability values with noise that has $U(0, 1)$ distribution. The corrupt predictions are a convex combination of the original prediction and the noise – we call the weight of the noise as the adversarial noise ratio. Given an adversarial noise ratio we calculate the mean Shapley value (with standard errors) for the adversarial and normally behaving classification trees in the ensemble.

5.4.2 Experimental findings. In Figure 5 we plotted the mean Shapley value of models which are adversarial and which are not in a scenario where half of the model owners mixed their predictions with noise. Even with a negligible amount of adversarial noise the Shapley values of adversarial models drop in the ensemble considerably. This implies that our method can be used to find adversarial models in a community contributed classification ensemble.

5.5 Scalability

We plotted the mean runtime of Shapley value approximations calculated from 10 experimental runs for an ensemble with $m = 2^5$ and dataset with $n = 2^9$ on Figure 6. All results are obtained with our open-source Shapley value approximation framework. These average runtimes of the approximation techniques are in line with the known and new theoretical results discussed in Sections 2 and 4. The precise estimates of Shapley values obtained with Troupe come at a runtime cost.

![Figure 6: The runtime of Shapley value approximation in ensemble games as a function of dataset size and number of classifiers in the ensemble.](image)

6 CONCLUSIONS AND FUTURE DIRECTIONS

We proposed a new class of cooperative games called ensemble games in which binary classifiers cooperate in order to classify a data point correctly. We postulated that solving these games with the Shapley value results in a measure of individual classifier quality. We designed Troupe a voting game inspired approximation algorithm which computes the average of Shapley values for every classifier in the ensemble based on a dataset. We provided theoretical results about the sample size needed for precise estimates of the model quality.

We have demonstrated that our algorithm can provide accurate estimates of the Shapley value on real world social network data. We illustrated how the Shapley values of the models can be used to create small sized but highly accurate graph classification ensembles. We presented evidence that complex models have an important role in the classification decisions of ensembles. We showcased that our framework can identify adversarial models in the classification ensemble.

We think that our contribution opens up venues for novel theoretical and applied data mining research about ensembles. We theorize that our model valuation framework can be generalized to ensembles which consist of multi-class predictors using a one versus many approach. Our work provides an opportunity for the design and implementation of real world machine learning markets where the payoff of a model owner is a function of the individual model value in the ensemble.
