### **CS 334 Machine Learning Final Project Report**

Zirui Deng, Yinfeng Wang

#### Abstract

In this project, we worked on the identification of credit card frauds. We used a dataset from Kaggle. The dataset is extremely unbalanced, as only 0.172% are fraud transactions. We chose recall score and area under the precision-recall curve as our model assessment metrics. As the dataset from Kaggle had already been preprocessed using PCA, we constructed a heatmap that showed low correlation between features. After that we split 30% of the dataset as our test set and kept the same ratio of fraud transactions in the training and test set.

We applied different machine learning classification models to the dataset and then computed metrics scores and plotted precision-recall curves of the models. We compared the results of the models and analyzed the reason why some models perform better than others for this project from aspects of our dataset and model algorithms. In the end we also reflected upon the limitations of our approach and acknowledged that future work could be done to make our results more precise and comprehensive.

#### Introduction

In this project, we aimed to address the problem of identifying credit card frauds. Nowadays people use credit cards anywhere they go. While credit cards certainly are a convenient way to make payments, for the past few years there have been numerous cases of fraudulent credit card transactions, and it is very important that credit card companies be able to recognize those frauds so that customers are not charged for items they did not purchase. Motivated by this reason, we decided to work on a project to detect credit card frauds.

In the project, we were dealing with a classification problem using the dataset collected from Kaggle, with class '0' for normal transactions and '1' for credit card frauds. Considering the unbalanced nature of the dataset, our approach to the problem was, after data preprocessing and feature selection, to experiment with different machine learning classifiers and then use these models as base learners to explore ensemble methods and see if they indeed work better according to our model assessment strategy.

The model assessment metrics used to evaluate the models should be suitable for the distribution of our dataset. Conventional measurements such as accuracy of prediction would not be sufficient to distinguish between models, as almost all of them have an accuracy above 99%. Recall that since 99.8% percent of our data were labeled '0', every model would have lots of true negatives (TN). We concluded that we should evaluate models by the true positives (TP), which means the area under the ROC curve would not be sufficient to evaluate models as well. So

instead of metrics learned in class, we decided to use the precision-recall metric. The formula for precision and recall are

$$P(Precision) = \frac{TP}{TP+FP}$$
 and  $R(Recall) = \frac{TP}{TP+FN}$ .

We observed that neither precision nor recall is influenced by TN, and both of them evaluate TP. This is exactly why we deemed precision-recall metric suitable for our data. Besides area under precision-recall curve (AUPRC), which is proposed by Kaggle, we also employed precision score, recall score and average precision score (AP) as other measurements of the model performances.

### **Background**

The original dataset has been collected and analyzed during a research collaboration of Worldline and the Machine Learning Group (<a href="http://mlg.ulb.ac.be">http://mlg.ulb.ac.be</a>) of ULB (Université Libre de Bruxelles) on big data mining and fraud detection. The data that we used contains only numeric input variables which were the result of a PCA transformation previously done by others. Due to confidentiality issues, the original features and more background information about the data are currently disclosed from the public. We noted that there are many approaches done by others on Kaggle. The one with the most upvotes was done by <a href="Janio Martinez">Janio Martinez</a>. He approached the problem by random undersampling with a 50/50 ratio of fraud and non-fraud and achieved a 93% recall score using Logistic Regression and SVM.

#### Methods

We decided to try out various classification models that were covered in class and compare their effectiveness in order to choose the optimal models for our task. We first took a look at KNN, which is the most basic classification models. Then we ran a Decision Tree classifier, another relatively basic learner, to see if it would do better than KNN. We also tried to see if a binary linear classifier could do the job, and we used Perceptron accordingly; we also picked Logistic Regression which is considered a generalized linear model for binary classification. Afterwards, we moved on to some more advanced models with higher-level classifiers. We first chose Complement Naive Bayes. Naive Bayes assumes that the features are independent, which is suitable for our case as we have checked previously. The reason we used Complement Naive Bayes in particular was that this adaptation of the standard multinomial Naive Bayes algorithm particularly fits for unbalanced datasets. SVM was also selected because this model uses margin for classification as well as optimization to find solution with fewer errors, and it has been proven to be one of the most efficient models.

Afterwards, we proceeded to try some ensemble methods which essentially take advantage of several learners to solve the same problem. We first employed two classic ensemble methods, Random Forest and Bagging with Decision Tree as the base learner. Here we decided to run two

models with similar tree structures so that we could make a reasonable comparison between these two ensembles as well. Other ensemble methods we picked were Voting and XGBoost. We used Logistic Regression, Decision Tree and Complement Naive Bayes as base learners for Voting with adjusted weights so as to see if Voting could indeed improve the performances of the three base models to a discernible degree. We also chose XGBoost as this is one of the most popular algorithms that is widely used by those who excelled in Kaggle competitions. We were curious to see if XGBoost could really generate results that would stand out among other models. Finally we turned to Neural Network. In particular, we chose Multilayer Perceptron (MLP). We wanted to see if using MLP could be a noticeable upgrade from Perceptron.

## **Experiments/Results**

The dataset contains transactions made by credit cards in September 2013 by European cardholders. It presents transactions that occurred in two days, during which there were 492 frauds out of 284,807 transactions included in the data. The dataset is highly unbalanced, with the positive class (frauds) accounting for only 0.172% of all transactions.

It contains variables that are the result of a PCA transformation. Features V1, V2, ... V28 are the principal components obtained from PCA; the only variables that have not been transformed with PCA are 'Time' and 'Amount'. Feature 'Time' denotes the seconds elapsed between each transaction and the first transaction in the dataset. 'Amount' is the transaction Amount. The 'Class' column is the response variable, and it takes value 1 in case of fraud and 0 otherwise.

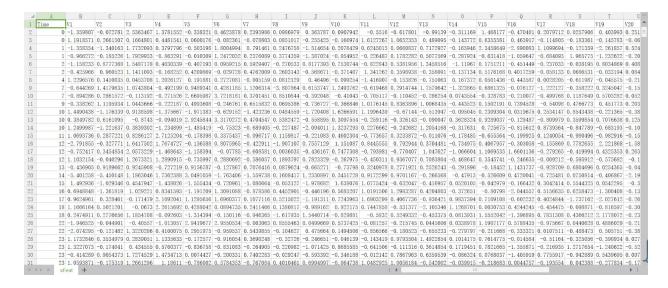


Figure 1: Screenshot of dataset

We conducted exploratory data analysis by checking the correlation between the features using the Pearson correlation matrix. By plotting the matrix with a heatmap that shows the correlation clearly, we saw from the graph that the features have really low correlation and are relatively independent with each other, meaning we could indeed use all features obtained from PCA. We

then extracted the 'Class' column from the dataset to establish a feature dataset and a target dataset. Afterwards we used holdout method, splitting the datasets into 70% training and 30% test sets. Because our data is highly unbalanced, we decided to use stratified sampling to make sure that the training and test data have the same distribution in the target variable as the original data. Random state was also used to ensure the same split every time. In addition, beforing running Complement Naive Bayes, we used a min-max scaler of range 0 to 1 on the feature datasets because Complement NB does not work with negative values.

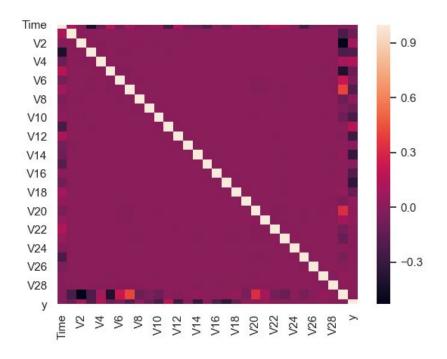


Figure 2: Heatmap of correlation

Finally, the models we selected were KNN, Decision Tree, Logistic Regression, Complement Naive Bayes, Voting, Bagging, Random Forest, XGBoost and MLP. Note that we did not include SVM because it took a really long time to converge, and it was hard for us to do further analysis. Also, our MLP model did not converge, as we could not find a parameter that would make it converge in a reasonable time. As a result, the scores obtained from MLP could not be considered entirely accurate, nor did they come off exactly impressive.

We started with the most basic model KNN and tuned the parameter 'n\_neighbors' with GridSearchCV and use 'precision' as the scoring parameter. The optimal value we got was 3. Then we tuned parameters for Decision Tree, and the parameters we chose were 'max\_depth' and 'min\_samples\_leaf'. With GridSearchCV we were able to find the optimal parameters: max\_depth = 7 and min\_samples\_leaf = 5. For Perceptron, we decided to set the parameter 'max\_iter' to be 1000 so that the model would converge. For Logistic Regression, we used the LogisticRegressionCV and set scoring as 'precision'. For ComplementNB, we didn't tune any parameter.

As stated before, Logistic Regression, Decision Tree and Complement Naive Bayes were selected as base learners for Voting. The weight we gave to Decision Tree was 2 while the other two had weight 1 as Decision Tree has the best performance among all three. For Logistic Regression we assigned 'max\_iter' to be 1000 to ensure convergence. Then using the optimal parameters that we obtained from tuning parameters of the Decision Tree classifier, along with Logistic Regression and Complement NB, we could run the Voting ensemble and get the improved results we desired. Also utilizing the optimal values from Decision Tree, we gave bagging another run and were delighted to see that the scores improved as well. For Random Forest, the parameters we tuned are 'max\_depth', 'min\_samples\_leaf', 'max\_features' and 'n\_estimators'. Again, we used GridSearchCV and the optimal value we got were max\_depth = 19, min\_samples\_leaf = 5, max\_features = 3, and n\_estimators = 30. Lastly, we tuned three parameters for XGBoost: 'max\_depth', 'n\_estimators' and 'learning\_rate'. Running GridSearchCV yielded the values that were optimal for these parameters: max\_depth = 6, n estimators = 350 and learning rate = 0.3.

Below is a table that shows how the models performed in terms of the four metrics that we decided on to compare these algorithms:

Model	Precision	Recall	AP	AUPRC
KNN	0.900	0.061	0.06	0.180
Decision	0.848	0.716	0.61	0.746
Tree				
Logistic Regression	0.833	0.507	0.42	0.707
Naive Bayes	0.706	0.730	0.52	0.639
Perceptron	0.000	0.000	0.00	0.003
Random Forest	0.940	0.720	0.68	0.813
Voting	0.913	0.709	0.65	0.794
Bagging	0.892	0.784	0.70	0.813

XGBoost	0.942	0.770	0.73	0.842
Neural Network*	0.678	0.784	0.60	0.695

Table 1: Metric scores of all models

To make the above outcomes easier to interpret, we conducted some visualization by plotting the precision-recall curves of these models in the same graph so that we could more conveniently and directly draw comparisons between the models' performances in order to judge which of them would be more suited for our task at hand. Remember that when one curve is placed above another, the above curve will have a larger area under the precision-recall curve (AUPRC) than the one below, and because AUPRC is one of the metrics employed by us to measure the performances of the models, the model corresponding to the curve that is above thus has a better performance than the model corresponding to the curve below. Here is what the graph looks like:

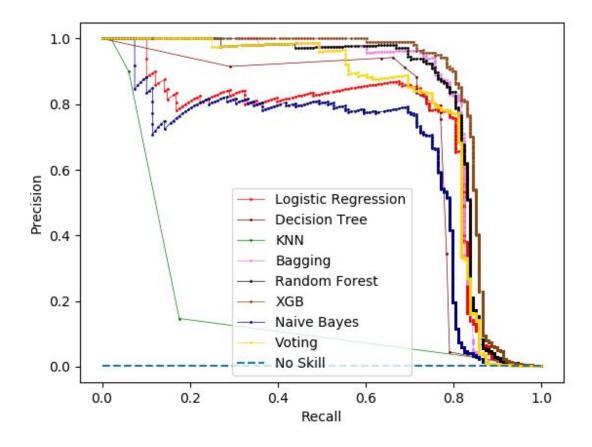


Figure 3: Precision-recall curves of models

Since we did not manage to get the MLP model to converge, we decided not to include it in the final graph. Perceptron was also left out of the group because its scores were fairly unsatisfactory

(to say the least). From the resulting graph above it is easy to see at first sight that one of the most used models nowadays XGBoost performed better than the others while the most fundamental model KNN did the poorest job of identifying credit card frauds. If we take a closer look at the remaining curves, it is not that difficult for us to see that both Random Forest and Bagging did a pretty good job, whereas Logistic Regression and Naive Bayes did not appear to be fit for the task. And in the middle we have Decision Tree and Voting. We were kind of surprised by how good Decision Tree did, considering it is a relatively basic algorithm.

#### **Discussion**

Note that precision score could not be regarded as persuasive enough for us to judge the performance of a model. A high precision score only means there are few false positives (FP). As mentioned before, all models had a high accuracy of prediction and lots of true negatives (TN). In this case, all models had few FPs. So we decided to rely on recall score, which gives the ratio of correct classifications of positive classes among all positive classes.

Among all the models we used for this project, KNN and Perceptron were the ones with the worst performance judging by our model assessment strategies. KNN has an average recall score of 0.06 while the recall score of Perceptron is almost zero, which means it failed to label any positive class correctly. We were curious about these results and believed that they were related to the logic and algorithm of these models. From our analysis, KNN simply categorizes data based on classes of nearest points. As our data is extremely unbalanced (0.172% of positive class), and we tuned the optimal 'n neighbors' with value 3, it is really unlikely that for a positive class, there are more than one positive classes among the three nearest points to it. This fact also suggests that the minority class in our dataset does not concentrate in an area of subspace. The bad performance of Perceptron could also be explained with its underlying mechanics. Perceptron is a kind of linear model that looks for a linear hyperplane to do binary classification. As we gave both classes an equal weight, the penalty for misclassifying a positive class was not significant enough to reflect such difference. We believed that giving the positive class more weights, or apply more margin to the positive class would yield a better result. This was similar to the mechanism of SVM, but the time to train an SVM model for this project was intimidating.

So we decided to try random undersampling as suggested by the most popular attempt on Kaggle. We used RandomUnderSampler from the imbalanced-learn API. There was a significant improvement in performances for both models after our update of data.

Model	Precision	Recall	AP	AUPRC
KNN	0.613	0.642	0.57	0.665
Perceptron	0.5	1	0.5	0.469

Table 2: Result of KNN and Perceptron after Undersampling

The recall score and AUPRC of KNN and Perceptron increased greatly. Perceptron had a recall score of 1 for this new balanced dataset which means it correctly labelled all positive classes.

Logistic Regression and Complement Naive Bayes have a medium performance just better than KNN and Perceptron. Logistic Regression was a generalized linear model. Although it has a sigmoid loss function  $\sigma(z) = \frac{1}{1 + exp(-z)}$ , z is still a linear function of input features. This nature would explain the normal performance of Logistic Regression as it is also imperfect to handle unbalanced dataset.

We could see the top five models all have tree structures: Decision Tree, Random Forest, Voting with Decision Tree having half of the weights, Bagging with Decision Tree as the basic learner, Random Forest and XGBoost. This gave us a basic idea that tree structures would be the priority for our project. They tackle our problem by learning a hierarchy of if/else questions and could force both classes to be addressed. Note that simple Decision Tree model or Voting did not perform much better than Logistic Regression and Naive Bayes. Ensemble methods like Bagging, Random Forest and XGBoost were evidently better than all of the rest models as Bagging has more estimators and Random Forest and XGBoost indeed employs randomness when finding a split in each node. They would be more likely to find and group the minority classes into an area of subspaces.

Also, with the data after random undersampling, our MLP model managed to converge. Its performance is better than simple Perceptron on the same data.

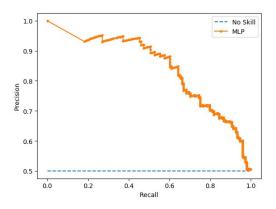


Figure 4: Precision-recall curve of MLP

Model	P	R	AP	AUPRC
MLP	0.881	0.601	0.73	0.843

Table 3: Metric Scores of MLP

### **Future Improvement**

While we did succeed in utilizing undersampling as a useful method to handle our unbalanced data and getting noticeable improvement in some models that previously did not perform very well, we are aware that there is still room for development through future research.

First, there are still a number of things we might be able to experiment with to improve upon the models we chose. To be more specific, we could try to refine linear models that operate on large margins like SVM so that we would afterwards have a better idea of the effectiveness of such models on dealing with our task of credit card fraud identification. We did not use SVM in our present research because running the model was too time-consuming; nevertheless, we could definitely could work on this algorithm in the future to see if it would have some value in helping us achieve our research goal.

Second, we could explore more in the ensemble category. During our research we chose such ensemble methods as bagging, Random Forest and XGBoost, and we also used voting which combined several base learners for the meta learner. However, there is much more to dig deep into. Methods like stacking and blending may very well be just as useful as some of the best models we selected and even more.

Last but not least, we recognized it is very important that our approach could be very well generalized, so another possible future task is to assess the generalizability of our strategies and algorithms. It would be ideal if our approach to identifying credit card frauds can be applied to other real-life cases with similarly unbalanced data; on the other hand, we might need to rethink our methodology if it cannot be used to handle other unbalanced data effectively.

#### Conclusion

We draw the conclusion that among all the models we discussed, Random Forest, Bagging with Decision Tree as the base learner and XGBoost are the best models for this project. The reason stemmed from their tree structures as well as their number of estimators and use of randomness when finding a split in each node. We believed that for other extremely unbalanced datasets, people should first consider these three models to deal with this problem. KNN and Perceptron did poorly for this project. They would be more efficient and accurate when the data is balanced. Logistic Regression and Naive Bayes had a medium performance. There is certainly much more we can do in the future, in particular regarding SVM and Neural Network.

# **Contributions**

We contributed equally on this project. We did the preprocessing of dataset together and split an even work distribution when tuning parameters, running all the models and recording the results.

Section	Contributor
Abstract	Yinfeng Wang
Introduction	Zirui Deng
Background	Together
Methods	Together
Experiments/Results	Together
Discussion	Together
Future Improvement	Zirui Deng
Conclusion	Yinfeng Wang

# Code

Link to our group Google Drive folder:

 $\underline{https://drive.google.com/drive/folders/1T06JpstXWo0Bp7mjQhbi-Up7-Bjo7hMX}$ 

# Reference

[1] Credit Card Fraud Detection. <a href="https://www.kaggle.com/mlg-ulb/creditcardfraud">https://www.kaggle.com/mlg-ulb/creditcardfraud</a>. Accessed: 2019-12-13.