COST MINIMISATION FOR CREDIT CARD FRAUD DETECTION USING NAÏVE BAYES AND RANDOM FOREST CLASSIFICATION

John McCabe, Kwun Ho Ngan[1]

[1]Department of Computer Science, School of Mathematics, Computer Science & Engineering, City University, London.

Problem Description and Motivation

The total loss on UK-issued card fraud has amounted to £566.0 million in 2017 [1] with 18.3 billion transactions made during the year. The aim of this project is to develop an optimised classification model that can detect card fraud and minimise the associated monetary loss from training a credit card fraud dataset available in the public domain.

Description of Dataset

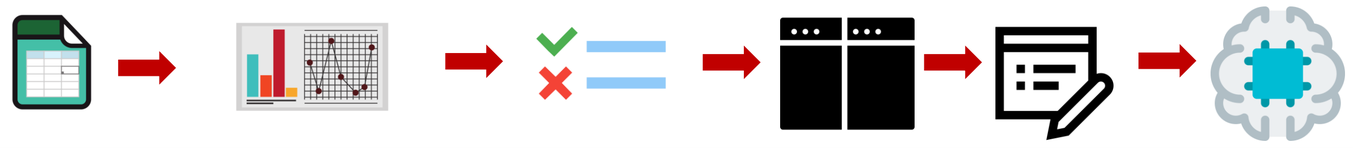
Dataset: Credit Card Fraud Detection [2]

Datapoints: 284,807 transactions

Predictors: Time, Amount and 28 Principal Components (Total: 30 features)

Outcome: Class

Data Pre-Processing Work Flow



Load Data	Exploratory Data Analysis	Feature Selection & Engineering	Train/Test Split	Re-sampling	Model Input
	Q-Q Plot Histogram Pair Matrix	Selection by feature differentiation Time-scale Conversion Log-norm Transformation	20% Holdout for out-of-sample testing between models.	Base Case x1 Under-sampling (5%, 10%, 50%) Over-Sampling (5%, 10%, 50%)	7x Training dataset of different fraud rate

Hypothesis Statement

Based on the outcome from Exploratory Data Analysis, Random Forest Classifier should perform better in this dataset given the imbalanced nature between legitimate and fraud transaction data point. Some features are found to be skewed and correlated within the fraud cases.

Comparison of Classification Models

	Naïve Bayes Classifier	Random Forest Classifier
Description	A supervised classification model based on Baye's Theorem by classifying labels through the learning of probability of event occurrence from available training data.	A supervised classification model by ensembling a series of Decision Trees of a random selected subset of features via a bagging method.
Features	• Fast Training • Fast Prediction • Interpretable results through posterior probability. • Posterior probability can be used for transfer models when new data is collected. • Few Hyperparameter Tuning Options for Model Optimisation. • Does not work well with outliers and non-Gaussian features. • Feature Scaling is not essential since it depends on the overall feature distribution.	• Fast Training (though takes ~5x longer than Naïve Bayes Classifier) • Fast Prediction. • Not easy to interpret the ensembled result (Interpret via individual tree level). • Model has to be reconstructed each time a new batch of data is collected. • Many Hyperparameter Tuning Options for Model Optimisation. • Outliers and non-Gaussian features do not generally impact classification. • Feature Scaling is not essential since it depends on the threshold for each tree split.

Results and Evaluation Analysis

Best Model: 10% Under-sampled Random Forest Classifier with a financial saving of 56%.

The final optimised model is based on the following cost minimisation criteria:

$$\min(Cost_{Fraud} \cdot Cases_{False\ Negative} + Cost_{Admin} \cdot Cases_{True\ Positive} + Cost_{Admin} \cdot Cases_{False\ Positive})$$

This evaluation criteria has similar effect as a comparison with F1 score where the precision and recall of a model are important. This however has an additional practical selection benefit to distinguish the effect of generating a false positive and false negative prediction.

Observations during Evaluation

- Random Forest Classifiers are able to minimise more false positive cases (i.e. legitimate transactions classified as fraud) comparing with Naïve Bayes Classifiers
- Without further feature engineering, most variations of NB/RF models yield about 20 false negative cases and 72 true positive cases. None of the tested hyperparameter appears to improve the performance in this regard.
- Over-sampled data set tend to perform better than under-sampled data set since it allows more legitimate transactions to be trained to minimise false positive prediction.
- A reduced subset of data with only features that have clear separation between the legitimate and fraud transactions (by minimal distribution overlap) yield at least equal or better prediction among the two classifiers.

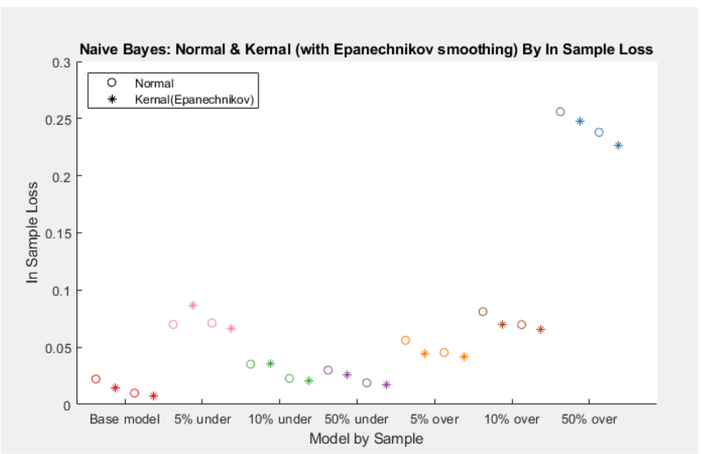


FIGURE 1: Hyperparameter Tuning for NB Classifier

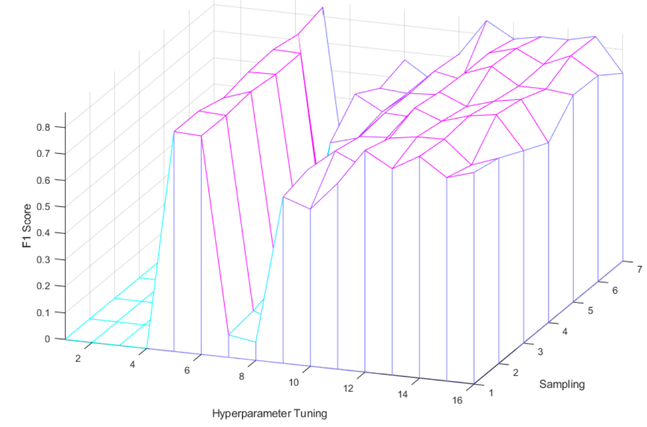


FIGURE 2: F1 Score of All tested models

ACKNOWLEDGEMENTS

The authors would like to thank Professor Artur Garcez and all teaching assistants for the coaching and support during the module. Your input are highly valued in the production of this work..

REFERENCES

[1] Fraud the Facts 2018, UK Finance.

[2] Dataset from Kaggle (Credit Card Fraud Detection), https://www.kaggle.com/mlg-ulb/creditcardfraud, Viewed on 15/11/2018.

[3] A. C. Bahnsen, A. Stojanovic, D. Aouada and B. Ottersten, Cost Sensitive Credit Card Fraud Detection using Bayes Minimum Risk, 12th International Conference on Machine Learning and Applications, pp. 333 – 338, 2013.

[4] M. Hossin and M. N. Sulaiman, A Review on Eavluation Metrics For Data Classification Evaluations, International Journal of Data Mining & Knowledge Management Process, Vol. 5 (2), pp. 1 – 11, 2015

[5] H. He, Y. Bai, E. A. Garcia, S. Li, ADASYN: Adaptive Synthetic Sampling Approach for Imbalanced Learning, IEEE International Joint Conference on Neural Networks, 2008.