Assignment 1 CDA

Tim van Rossum, 4246306
Michiel Doesburg,

May 4, 2018

1   A visualization of the data

For the visualization part of this assignment, we first started out by making bar plots of different kinds, but eventually settled for the scatterplot as seen in figure 1. This scatterplot uses the amount of Eurocent spent per transaction, to allow for better comparisons to be made, as there were five different currencies in the dataset. Exchange rates of April 25, 2018 were used. As can be seen from the scatterplot, there are basically no fraudulent transactions where more than 800 Euro was spent, while there are many benign transactions where more than 800 Euro was spent. Other visualizations we made included the ratio of fraudulent versus non-fraudulent transactions per country and per card issuer. Notable observations were that most nearly all fraudulent transactions come from Mexico and Australia (nearly 90 percent), while these two countries are responsible for very few non-fraudulent transactions. McCredit is responsible for significantly more fraudulent transactions than non-fraudulent. The inverse being true for visadebit, which accounts for roughly 60 percent of benign transactions, yet only 10 percent of fraudulent ones.
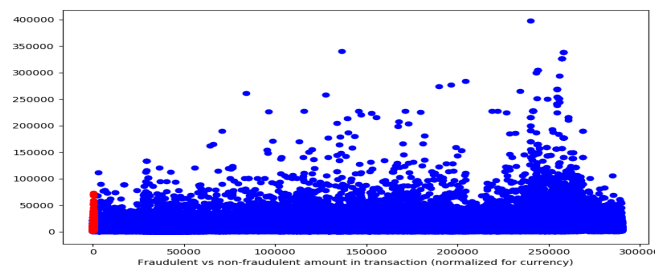

Figure 1: A scatterplot of the amount of money spent in the sampled transactions. A red dot indicates a fraudulent transaction (these are only at the very left of the plot due to very little fraudulent transactions existing), while a blue dot indicates a benign transaction.

2 Applying SMOTE to the data

Because we used Python for this assignment with `scikit-learn`, we used SMOTE as implemented in the package `imblearn`. The `fraud_detection.py` script already preprocessed the data in such a way that applying SMOTE to it was very easy, as the implementation only needed the data and the class labels, and both were already generated by the script. The general steps of preprocessing are:

- Remove data with the "Refused" label (as that is data where we cannot be certain whether or not it is fraudulent)

- Remove the ID and booking date of the transaction, as these are not necessary.

- Transform the mail identifiers, IP identifiers etc. to simply the number that they use.

The classifiers that we used were the random forest classifier, the 5-NN classifier, and the logistic classifier. These were chosen to represent both linear and non-linear classifiers, as well as parametric and non-parametric classifiers (as NN is deemed a non-parametric classifier). The ROC curves are shown in figure 2.
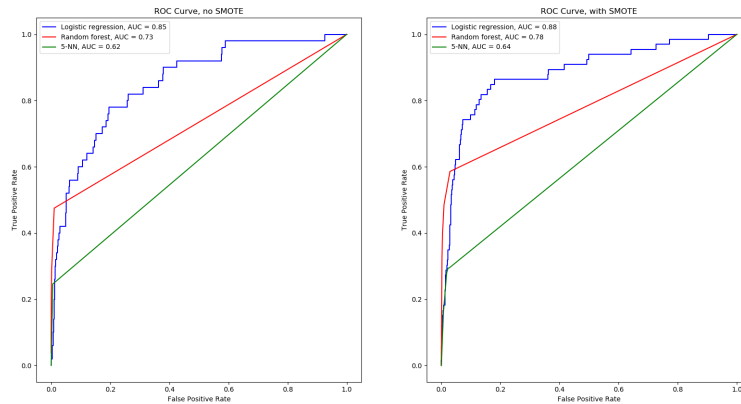

Figure 2: Caption of ROC curves.

3 The black box and white box classifier

For the white box classifier we took a look at several features of the data: issuer country code; transaction variant code, shopper interaction, card verification, cvc response, account code and card issuer identifier. We wrote a small script which, for the fraudulent transactions only, gathered the ranges of values that these features take. Our classifier works quite simply: if for each feature there is a fraudulent transaction which has the same value as a transaction, that transaction is labelled as fraudulent. Althouth this is a very rough approach, it seems to work quite well on the test data. This approach produces the following results:

TP: 155
FP: 5
TN: 236686
FN: 190

For the white box classifier, we will use the following decision rules to determine whether or not a transaction is fraudulent:

- The transaction originates from either Mexico or Australia (as these two countries have about two-third of the total fraudulent transactions).

- The card issuer identifier is between 401795 and 558320, both inclusive. This is the range in which fraud was detected.

- The card type used was mccredit, visaclassic or visadebit. These three card types are used in about two thirds of the fraud cases.

- In the case of Australia, for a transaction to be classified as fraudulent, the currency used must be the Australian dollar, the merchant's webshop value should be APACAccount, the the card verification code must be supplied, the amount spent must be between 250 AUD and 350 AUD, the interaction should be via E-commerce, and the CVC response code should be 0.

- In the case of Mexico, for a transaction to be classified as fraudulent, the currency used must be the Mexican peso, the merchant's webshop value should be MexicoAccount.

For the black box classifier, we will be using the random forest classifier, as this classifier tended to perform better, especially on SMOTEd data. It is also a classifier that has been shown to perform better in the papers