**Einleitung**

Derzeit stellen unausgeglichene Datensätze eine erhebliche Herausforderung im Bereich des maschinellen Lernens und des Data Minings dar. Denn die herkömmlichen Klassifizierungsverfahren neigen in der Regel dazu, die Mehrheitsklasse zu bevorzugen, welche bei einem binären Klassifizierungsproblem oft ein Vielfaches an Instanzen gegenüber der Minderheitsklasse besitzt. Hierdurch wird der Klassifikator in seiner Vorhersagefähigkeit, die Minderheitsinstanzen korrekt zu erkennen, stark beeinträchtigt, kann jedoch trotzdem eine hohe Accuracy aufweisen. Die Minderheitsklasse kann dabei auch völlig unerkannt bleiben. Diese Thematik ist insbesondere bei der Erkennung betrügerischer Transaktionen in Banken, Kreditrisikobewertung oder Erkennung von Firewall-Eingriffen von hoher Bedeutung. Aufgrund dieser universellen Existenz von unausgewogenen Datensätzen wurden bereits viele Vorverarbeitungsmethoden vorgeschlagen, um die Imbalance zu bewältigen. Oversampling ist eine vielversprechende Technik für unausgewogene Datensätze, die neue Minderheiteninstanzen erzeugt, um den Datensatz auszugleichen. Unter den Oversampling-Methoden ist die Synthetic Minority-Oversampling-Technique (SMOTE) eine der bekanntesten Methoden, die künstliche Minoritätsinstanzen durch lineare Interpolation erzeugt. Eine jüngst veröffentlichte Adaption dessen liefert im Paper „ASN-SMOTE: a synthetic minority oversampling method with adaptive qualified synthesizer selection“ von Yi Xinkai et al. (2022) vielversprechende Ergebnisse, weshalb dieser Algorithmus im Folgenden auf dem Creditcard Datensatz angewendet wird. Weiterhin wird seine Performance mithilfe zweier geeigneter Classifier und den Ergebnissen des originalen SMOTE Algorithmus untersucht. Dafür wird nach der Data Exploration und Anwendung des SMOTE im 1. Kapitel die Funktionsweise des ASN-SMOTE sowie die Unterschiede zum ursprünglichen Algorithmus in Kapitel 2 erläutert. Anschließend werden die verwendeten Classifier und das Performancemaß in Kapitel 3 sowie die gewählte Cross-Validation im 4. Kapitel präsentiert. Darauf folgt in Kapitel 5 und 6 eine Methode des Undersamplings und die Durchführung der Hyperparameteroptimierung. Abschließend werden die Ergebnisse des ASN-SMOTE in Kapitel 6 analysiert, bevor ein Ausblick mit weiteren Ideen und Forschungsfragen folgt. Der Code des entsprechenden Abschnitts ist zur Nachvollziehbarkeit in der Programmiersprache R an jedes Kapitel angehängt.

1. **Data Exploration**

Der zu behandelnde Datensatz Creditdata beinhaltet europäische Kreditkartentransaktionen von September 2013 im CSV-Format und besitzt pro Transaktion 31 Features/Spalten, wobei die letzte binäre Spalte die Target darstellt. Diese definiert, ob ein Sample Fraud (1) oder kein Fraud (0) ist. Das Ziel hierbei ist es ein Machine Learning Modell zu trainieren, welcher Kreditkartenbetrug erkennen soll, um die Kunden vor unautorisierten Belastungen zu schützen. Die Daten sind ausschließlich numerisch und abgesehen von Time und Amount aus Datenschutzgründen mit PCA transformiert worden. Zu Beginn werden die notwendigen Packages geladen sowie die Working Directory in den Ordner gesetzt, worin sich der Creditdata Datensatz befindet und mit read.csv eingelesen. Anschließend wird eine NA-Analyse durchgeführt und einige Statistiken der einzelnen Spalten berechnet. Die Imbalance des Datensatzes wird deutlich, wenn wir die Anzahl der Minority Samples mit den 284.315 der Majority vergleichen. Denn es befinden sich lediglich 492 Fraud Samples in Creditdata, was einem Prozentsatz von 0,17% entspricht. Dies deutet auf eine extreme Imbalance zwischen Majority und Minority hin und macht eine Preprocessingmethode umso notwendiger. Aufgrund der hohen Imbalance wird ein 90 zu 10 Split der Daten in Trainings- und Testdatensatz durchgeführt, worauf eine Trennung der Features von der Target Variable folgt. Da das Feature Time als nicht aussagekräftig genug erscheint, wird dieses aus dem Datensatz entfernt und ebenfalls ein Scaling der Spalte Amount vorgenommen, da diese nicht mit PCA transformiert wurde. Dies geschieht in Trainings- und Testdatensatz separat, um den Mittelwert und die Standardabweichung des Testdatensatzes nicht mit in den Trainingsdatensatz aufzunehmen, was andernfalls zu Overfitting führen würde. Beim Korrelationsplot der Features mit der Target Variable fallen einige positive als auch negative Korrelation beim Feature Amount beispielsweise mit V2 und V7 auf. Die Target Value weist z.B. mit den Features V12, V15 und V17 lediglich einige niedrige negative Korrelation auf. Dies liegt insbesondere an der PCA Transformation, welche in Voraus durchgeführt wurde. Aus diesem Grund werden keine Features selektiert.

1. **SMOTE und ASN-SMOTE**

**2.1 Anwendung des SMOTE Algorithmus**

Im Anschluss an die Data Exploration wird der in R bereits implementierte SMOTE Algorithmus aus dem Package smotefamily auf den Trainingsdatensatz angewendet, um eine Balance im Datensatz herzustellen. Nach der Generierung von 255.228 synthetischen Trainingsdaten beträgt der Anteil der Minority Samples im Train Set 49,97%. Beim Vergleich der Visualisierungen mit den Features V1 und V2 wird die Funktionsweise des SMOTE Algorithmus mit linearer Interpolation durch die geraden Linien, welche die synthetischen Daten ziehen, deutlich.

**2.2 ASN-SMOTE**

Allerdings können unsachgemäß erzeugte Minority Samples das Lernen des Classifiers auch beeinträchtigen und sich negativ auf ihn auswirken. Da im originalen SMOTE Algorithmus sowohl alle Minority Instanzen als auch alle k-nearest neighbors gleich behandelt werden und somit zur Generierung synthetischer Datenpunkte verwendet werden, kann dies zu einem Verschwimmen der Entscheidungsgrenze bzw. Überlappen der Feature Spaces führen. Durch die synthetischen Daten im Feature Space der Majority Class, wird es für ein Modell schwierig die beiden Klassen zu unterscheiden. Auf dieses Problem zielt der einfache und effektive Ansatz des ASN-SMOTE ab, welcher ebenfalls auf der k-Nearest-Neighbors und SMOTE-Technologie basiert. Dieser lässt sich in drei Algorithmen unterteilen, wobei der erste als Noise-Filtering bezeichnet wird. Hierbei wird für jede Minority Instanz die euklidische Distanz zu allen anderen Datenpunkten berechnet und lediglich der nächste Nachbar betrachtet. Sollte dieser zur Majority gehören, wird die gerade betrachtete Minority Instanz als Noise klassifiziert und im weiteren Verlauf nicht als Synthesizer für die Datengenerierung verwendet. Sollte der nächste Nachbar ebenfalls zur Minority gehören, ist die betrachtete Minority Instanz qualifiziert für die Generierung synthetischer Daten. Dies dient zur Filterung von Noise und Instanzen entlang der Entscheidungsgrenze. Im Anschluss folgt der Algorithmus zur adaptiven Nachbarauswahl, wobei für die k nächsten Nachbarn erneut die euklidische Distanz berechnet wird. Befindet sich darunter eine Majority Instanz, werden nur diejenigen als Nachbar für die Synthese genutzt, welche eine geringere Distanz als die nächste Majority Instanz aufweisen. Alle anderen Nachbarn werden als unqualifiziert markiert und nicht für die Datengenerierung mit der betrachteten Minority Instanz verwendet. Der dritte Algorithmus dient zur Erstellung der Samples, wobei anfangs die Anzahl der notwendigen neuen Instanzen für jedes Minority Sample bis zur optimalen Balance berechnet werden. Daraufhin folgt die Anwendung des SMOTE Algorithmus, welcher die synthetischen Daten mithilfe der linearen Interpolation erstellt. Dabei wird die euklidische Distanz zwischen der Synthesizer Minority Instanz und einem zufällig ausgewählten Nachbar der k nächsten Nachbarn (bei ASN: nur qualifizierten k nächsten Nachbarn) mit einer Zufallszahl zwischen Null und Eins multipliziert und zur Synthesizer Instanz addiert. Anschließend wird zu jeder erstellten Instanz die Target Variable (1) hinzugefügt und die synthetischen Daten an den Trainingsdatensatz angehängt. Die Vorteile des neuen Ansatzes sind dabei die Effektivitätssteigerung durch das Filtern von Noise sowie die Feature Spaces daran zu hindern sich zu überlappen. Die Wirksamkeit dieses modernen ASN-SMOTE Algorithmus wurde mit 24 unausgewogenen Datensätzen im Originalpaper getestet und zeigte durchweg positive Ergebnisse im Vergleich mit anderen namhaften SMOTE Adaptionen. Die Imbalance der 24 Datensätze lag dabei zwischen 1,82% und 41,4%, weshalb die folgenden Fragen aufkommen: Funktioniert der ASN-SMOTE auch beim Creditdata Datensatz, welcher eine deutlich höhere Imbalance von 0,17% aufweist? Oder ist möglicherweise ein vorausgezogenes Undersampling notwendig? Bei der Anwendung des Algorithmus auf den gegebenen Datensatz, zeigt sich, dass 82 der lediglich 442 Minority Samples im Trainingsdatensatz als unqualifiziert klassifiziert werden, wodurch dem Classifier das Lernen noch mehr erschwert wird. Bei der Analyse von höheren Werten für den Hyperparameter k wird deutlich, dass nur die wenigsten Minority Instanzen 30 nächste Nachbarn aus der eigenen Klasse oder mehr besitzen und keine mehr als 80. Daher wird beim Tuning ein höheres Augenmerk auf niedrige Wert für k gelegt und dieser Bereich feiner unterteilt als hohe Werte für k. Aufgrund von Unstimmigkeiten im ASN-Paper wurde „n“ die Anzahl der zu generierenden Samples pro qualifizierter Minority Instanz sowohl als Inputparameter festgelegt als auch in der Funktion selbst „n\_opt“ berechnet. Durch Auskommentieren der Codezeile „n <- n\_opt“ kann n als Eingabewert verwendet werden und andernfalls wird jenes n gewählt, welches zur optimalen Balance im Datensatz führt. Beim Plot der Features V1 und V2 wird fällt anhand der zwei gekennzeichneten Punkte der Unterschied zum SMOTE Ansatz deutlich auf, da die vom ersten Algorithmus als Noise klassifizierte blaue Minority Instanz nicht für die Generierung synthetischer Daten verwendet wird. Zudem wählt der Algorithmus zur Nachbarauswahl den zweiten gekennzeichneten Punkt der Majority Class nicht als qualifizierten Nachbar aus. Das Verhalten des ASN ist bei Zweiterem aber möglicherweise ungünstig, da es sich hierbei um einen Ausreißer der Majority handeln könnte, welcher im Feature Space der Minority liegt.

1. **Verwendete Classifier und Performancemaß**
   1. **Verwendete Classifier**

Um für das Testdatenset Vorhersagen treffen zu können, müssen wir erst ein Modell aufstellen und dieses tunen. Hierbei entscheiden wir uns für die Machine Learning Modelle der Logistischen Regression und des Random Forest. Die Logistische Regression eignet sich beispielsweise gut für die Schätzung der Wahrscheinlichkeiten von binären oder kategorialen abhängigen Variablen. Der grundlegende Ansatz der logistischen Regression besteht darin, dass eine Sigmoid-Funktion auf eine lineare Kombination der Features angewendet wird. Die Sigmoid-Funktion transformiert den linearen Ausdruck in einen Wert zwischen 0 und 1, der als Wahrscheinlichkeit interpretiert werden kann. Zudem findet eine Regularisierung statt, welche mit dem Hyperparameter C festgelegt wird. Dieser ist auch der einzige zu tunende Parameter im Modell, wodurch eine Cross-Validation mit geringerem Rechenleistung durchgeführt werden kann. Jedoch könnte die vom Modell angenommene lineare Beziehung zwischen den Features einen Nachteil darstellen. Im Bezug auf den Random Forest ist zu wissen, dass er zu den Ensemble-Lernverfahren gehört und für Klassifikations- und Regressionsaufgaben verwendet wird. Er besteht aus einer Kombination von Entscheidungsbäumen, die unabhängig voneinander trainiert werden. Dabei wird jeder Baum auf einer zufälligen Stichprobe der Trainingsdaten trainiert und betrachtet auch nur eine zufällige Teilmenge der verfügbaren Features. Dies hilft dem Modell, um Overfitting zu vermeiden und gut verallgemeinern zu können. Bei einer Klassifikationsaufgabe ist die Vorhersage üblicherweise eine Mehrheitsentscheidung der Bäume. Die Vorteile dieser Methode sind, dass der Random Forest problemlos mit großen Datenmengen arbeiten kann und nicht dazu neigt die Trainingsdaten auswendig zu lernen. Zudem schneidet er in der Praxis oft besser ab als andere Classifier. Beim Tuning sind jedoch deutlich mehr Hyperparameter zu optimieren, wodurch ein großer Rechenaufwand notwendig ist und das Modell ist meist schwieriger zu interpretieren als einfachere Verfahren, wie z.B. die Logistische Regression.

**3.2 Performancemaß**

Die Leistung der Algorithmen des maschinellen Lernens wird in der Regel anhand einer Konfusionsmatrix bewertet und die Vorhersagegenauigkeit definiert als Accuracy = (T P + T N)/(T P + F P + T N + F N). Dabei ist die Fahlerrate 1 – Accuracy. Dies gilt jedoch nur im Zusammenhang mit ausgeglichenen Datensätzen und gleichen Fehlerkosten. Denn beim betrachteten Datensatz würde sogar ein Modell, welches immer die Majority prognostiziert, eine Accuracy von über 99% erreichen. Daher verwenden wir beim Creditdata Datensatz mit ungleichen Fehlerkosten, die Receiver Operating Characteristic Curve (ROC-Curve) und die Area under the Curve (AUC), um die Performance der Logistischen Regression und des Random Forests zu bestimmen. Hierbei wird auf der X-Achse die False-Positive-Rate %F P = F P/(T N+F P) und auf der Y-Achse die True-Positive-Rate %T P = T P/(T P +F N) dargestellt. Der ideale Punkt auf der ROC-Kurve wäre (0,100), d. h. alle positiven Samples werden richtig klassifiziert und keine negativen Beispiele werden falsch als positiv klassifiziert. Die Linie y = x stellt das Szenario einer zufälligen Schätzung der Klasse dar. Zudem ist die Fläche unter der ROC Kurve (AUC) ein nützliches Maß für die Leistung des Klassifikators, da es unabhängig vom gewählten Entscheidungskriterium und den vorherigen Wahrscheinlichkeiten ist.