**Untersuchung und prototypische Umsetzung eines Lifelong Deep Neural Network Algorithmus**

|  |  |
| --- | --- |
|  | |
| Masterarbeit 3062 | |
| An der Universität Stuttgart vorgelegt von  **Simon Kamm** | |
| Elektro- und Informationstechnik | |
|  | |
| Prüfer: | Prof. Dr.-Ing. Michael Weyrich |
| Betreuer: | Benjamin Maschler, M.Sc. |
| 29.10.2019 | |

Hinweise zu dieser Vorlage:

Allgemein

Die Ausarbeitung ist ein wesentlicher Bestandteil Ihrer Prüfungsleistung. Sie können sich gerne an anderen Ausarbeitungen orientieren oder Ihre Gliederung mit Ihrem Betreuer besprechen. Die konkrete inhaltliche Gestaltung sollte jedoch Ihre eigene Leistung sein und über ein bloßes Zusammenkopieren der Zwischendokumente hinausgehen. Ihr Ziel sollte eine in wissenschaftlicher Sprache verfasste Darstellung der wesentlichen Schritte und Ergebnisse Ihrer Arbeit sein, die es einem Außenstehenden ermöglicht, nachzuvollziehen, warum Sie wozu welche Entscheidungen getroffen haben.

Bitte ersetzen Sie Platzhalter in eckigen Klammern (z. B. „<Abgabedatum>“) durch die korrekte Information und löschen Sie anschließend die eckigen Klammern (z. B. „01.01.2017“).

Bitte entfernen Sie alle blauen Anmerkungen (sowie diese Hinweis-Seite).

Bitte nutzen Sie soweit möglich Word-Funktionen (z. B. zur Erstellung von Verzeichnissen, Beschriftungen von Abbildungen und Tabellen, Querverweise)

Titelseite

Bitte schreiben Sie die Art der Arbeit aus (z. B. „Masterarbeit“ statt „MA“).

Bitte entfernen Sie den Inhalt der Zeile „Externer Betreuer“, wenn Sie keinen externen Betreuer haben.

Bitte entfernen Sie das Textfeld „Diese Arbeit ist vertraulich.“, wenn Ihre Arbeit nicht vertraulich ist.

# **Inhaltsverzeichnis**

Inhaltsverzeichnis iii

Abbildungsverzeichnis v

Tabellenverzeichnis vii

Abkürzungsverzeichnis viii

Glossar ix

Zusammenfassung x

Abstract xi

1 Einleitung 12

2 Theoretische Hintergründe 14

2.1 Deep Learning 14

2.2 Kontinuierliches Lernen 22

2.3 Inkrementelle Klassifikatoren 28

2.4 Verteiltes Lernen 33

3 Lifelong Deep Neural Network Algorithmus 39

3.1 Beschreibung 39

3.1.1 Kontinuierliches Lernen 42

3.1.2 Verteiltes Lernen 43

3.2 Vorteile 44

3.3 Nachteile 45

3.4 Zusammenfassung und Vergleich zu klassischen Ansätzen 45

4 Konzeption 47

4.1 Modul A 47

4.1.1 AlexNet 47

4.1.2 VGG 48

4.1.3 ResNet 50

4.1.4 GoogLeNet/Inception 53

4.1.5 MobileNet 54

4.2 Modul B 55

4.3 Zusammenfassung 58

4.3.1 Modul A 58

4.3.2 Modul B 60

4.3.3 Lifelong DNN Algorithmus 62

5 Aufbau der Evaluierung 64

5.1 Datensätze 64

5.2 Evaluierungskriterien 65

5.3 Evaluierungsfälle 66

6 Evaluierung und Ergebnisse 68

6.1 Hyperparameter-Optimierung Modul B 69

6.2 Einfluss der Anzahl von Trainingsdaten 75

6.3 Finale Ergebnisse 79

6.3.1 Kontinuierliches Lernen 80

6.3.2 Verteiltes Lernen 82

6.4 Einfluss von Konsolidierungsschritten 84

6.5 Gesamter ImageNet-Datensatz 88

7 Demonstrator 93

8 Zusammenfassung und Ausblick 94

Literatur 95

Erklärung 99

# Abbildungsverzeichnis

Abbildung 1: Verhältnis von verschiedenen Lernansätzen zu Machine Learning 14

Abbildung 2: Generelle Problemstellung für maschinelles Lernen 15

Abbildung 3: Einzelnes Neuron in einem *Feedforward Neural Network* 16

Abbildung 4: Neuronen-*Layer* 17

Abbildung 5: Neuronen-*Layer* in komprimierter Darstellung 17

Abbildung 6: Vorwärts-Pfad durch ein Netzwerk 20

Abbildung 7: Error Backpropagation durch ein Netzwerk 21

Abbildung 8: Erlernen neuer Aufgabe B und mögliche Folgen 23

Abbildung 9: Einfluss von EWC auf Parameteranpassungen [18] 24

Abbildung 10: Schematische Darstellung der Dual-Memory Methode 26

Abbildung 11: Darstellung der drei Continual Learning Szenarien am Beispiel von Split MNIST [13] 27

Abbildung 11: Ablaufdiagramm des Betriebs eines ART-Netzwerk 32

Abbildung 12: Modul A und Interface zu Modul B 40

Abbildung 13: Graphische Darstellung des L DNN A 41

Abbildung 14: Beispielhaftes Szenario mit mehreren Endgeräten und einem zentralen Server 41

Abbildung 15: Modelarchitektur des AlexNet [34] 48

Abbildung 16: Beispielhafter Residual Block [38] 51

Abbildung 17: Beispielhafte Architektur VGG-19 (links), Standard-Architektur (mitte), ResNet (rechts) [38] 52

Abbildung 18: Inception-Modul [39] 53

Abbildung 19: Schematische Übersicht über MobileNet-V2 Architekture [43] 55

Abbildung 20: Architektur des SFAM-Netzwerks 61

Abbildung 21: Gesamtarchitektur L DNN Algorithmus 62

Abbildung 22: MNIST-Bild vor Bild-Augmentation 68

Abbildung 23: MNIST-Bild nach Augmentation 69

Abbildung 24: Ergebnisse der Gitter-Suche für und auf Basis des Split-MNIST Datensatzes 72

Abbildung 25: Ergebnisse der Gitter-Sucher für und auf Basis des ImageNet-10 Datensatzes 72

Abbildung 26: Speicherbedarf von Modul B in Abhängigkeit von für Split-MNIST 74

Abbildung 27: Speicherbedarf von Modul B in Abhängigkeit von für ImageNet-10 74

Abbildung 28: Klassifikationsgenauigkeit über die Anzahl an Trainingsbildern Split-MNIST 76

Abbildung 29: Klassifikationsgenauigkeit über die Anzahl an Trainingsbildern ImageNet-10 77

Abbildung 30: Speicherbedarf Modul B über die Anzahl an Trainingsbildern Split-MNIST 77

Abbildung 31: Speicherbedarf Modul B über die Anzahl an Trainingsbildern ImageNet-10 78

Abbildung 32: Klassifikationsgenauigkeit für unterschiedliche Konsolidierungsmethoden 85

Abbildung 33: Klassifikationsgenauigkeit für unterschiedliche Konsolidierungsmethoden 85

Abbildung 34: Klassifikationsgenauigkeit bei ImageNet für unterschiedliche inkrementelle Lernalgorithmen 89

Abbildung 35: Klassifikationsgenauigkeit bei ImageNet mit unterschiedlicher Anzahl an inkrementellen Schritten 89

# Tabellenverzeichnis

Tabelle 1: Übersicht über Verteilte Deep Learning Methoden 34

Tabelle 2: Kategorisierung von *Federated Learning* 37

Tabelle 3: Übersicht der behaupteten Vorteile des L DNN Algorithmus gegenüber traditionellen DNNs 44

Tabelle 4:VGG-Netzwerk Architekturen [37] 49

Tabelle 5: Vergleich von VGG-16 und VGG-19 50

Tabelle 6: Vergleich von ResNet-50 und ResNet-100 52

Tabelle 7: Depthwise Separable vs. Full Convolution MobileNet [41] 54

Tabelle 8: Übersicht aller vorgestellten DNNs für Modul A 58

Tabelle 9: Architektur MobileNet-V2 [42] 60

Tabelle 10: Klassifikationsgenauigkeit verschiedener Algorithmen auf Split-MNIST 80

Tabelle 11: Klassifikationsgenauigkeit des verteiltem L DNN Algorithmus auf Split-MNIST 83

Tabelle 12: Klassifikationsgenauigkeit des verteiltem L DNN Algorithmus auf ImageNet-10 83

Tabelle 13: Vergleich von Speicherbedarf und finaler Klassifikationsgenauigkeit für unterschiedliche Methoden der Konsolidierung Split-MNIST 86

Tabelle 14: Vergleich von Speicherbedarf und finaler Klassifikationsgenauigkeit für unterschiedliche Methoden der Konsolidierung ImageNet-10 86

Tabelle 15: Finale Klassifikationsgenauigkeiten ImageNet 90

Tabelle 16: Relativer Erhalt der Klassifikationsgenauigkeit auf ImageNet 91

# Abkürzungsverzeichnis

Konvention: Abkürzung selbst nicht fett, dafür aber in der Langform die Buchstaben fett, die die Abkürzung ergeben.

|  |  |
| --- | --- |
| ASCII | **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange |

# Glossar

Formatvorlage: IAS\_Glossary (Hauptbegriff fett)

|  |  |
| --- | --- |
| **Aktuator** | Einheit zur Umsetzung von Stellinformation tragenden Signalen geringer Leistung in leistungsbehaftete Signale einer zur Prozessbeeinflussung notwendigen Energieform. |

# Zusammenfassung

Formatvorlage: Standard (maximal 2000 Zeichen)

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum.

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

**Schlüsselwörter:** Hier bitte (ca. 6 bis 12) Schlüsselwörter auflisten.

# Abstract

Formatvorlage: Standard (maximal 2000 Zeichen, Übersetzung der Zusammenfassung)

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum.

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

**Key Words:** *Hier bitte (ca. 6 bis 12) englische Schlüsselwörter auflisten.*

# Einleitung

Danteschutz ist heutzutage ein wichtiger Aspekt, der in neuen Anwendungen nicht missachtet werden kann. Sowohl bei persönlichen Daten, die beispielsweise auf einem Smartphone gesammelt werden, als auch bei industriellen Daten wie von einer Produktionsanlage, muss der Schutz dieser Daten gewährleistet werden. Der Schutz von diesen Daten steht bisher weitgehend in Widerspruch zu Multitaskingfähigen Machine Learning Algorithmen. Durch diesen Widerspruch wird eine flächendeckende Nutzung von KI-Methoden häufig verhindert. Dennoch ist der Wunsch nach einem breiteren Einsatz von KI-Methoden vorhanden, da dadurch viele neue Anwendungen erschlossen werden können oder bestehende Anwendungen weiter verbessert werden können.

Beispielhaft kann die Anwendung „*Predictive Maintenance*“ gesehen werden. Dabei werden auch heute schon Machine Learning Algorithmen eingesetzt, um mögliche Ausfälle von Maschinen vorherzusagen und vorbeugende Instandhaltungsarbeiten zu ermöglichen, die wiederum lange und teure Ausfallzeiten verhindern. Dafür werden vortrainierte neuronale Netze oder andere fixe Machine Learning Algorithmen genutzt. Durch kontinuierlich („*Continual*“) und verteilt („*Distributed*“) lernende Algorithmen könnte der Einsatz von diesen Algorithmen sowie deren Performanz weiter gesteigert werden. Diese Algorithmen sind in der Lage während dem Betrieb kontinuierlich weiter zu lernen und können so auf abweichende Ereignisse reagieren, die vorher nicht bekannt waren und somit nicht erlernt werden konnten. Durch verteiltes Lernen können sich gleiche Maschinen zudem austauschen, wodurch die Information über einen Vorfall 1, den Maschine A gesehen und erlernt hat, an Maschine B weitergegeben werden kann. Wie bereits beschrieben, brauchen bisherige Ansätze dafür jedoch den Austausch von Daten sowie die Speicherung dieser Daten, was bei Echtzeit-Anwendungen eine erhebliche Speicher- und Rechenleistung erfordert. Zudem kann es auch schlicht verboten bzw. unerwünscht sein, gesammelte Daten von Maschine A and Maschine B weiterzugeben, wenn diese bei einem Wettbewerber im Einsatz ist. Dasselbe gilt für private Anwendungen wie beispielsweise medizinischen Anwendungen. Mithilfe von gesammelten Daten von Fitnessuhren könnten Netzwerke Krankheiten oder Symptome von Krankheiten frühzeitig erkennen. Jedoch ist es in der Regel vom Anwender nicht erwünscht, dass diese persönlichen Daten auf einem zentralen Server gespeichert werden um dort ein neuronales Netzwerk zu trainieren.

Sogenannte Lifelong Deep Neural Network Algorithmen (L DNN A) können das Potenzial haben, diesen Widerspruch aufzulösen, indem sie verteiltes und kontinuierliches Lernen ohne den Austausch von Rohdaten ermöglichen und dabei auch auf mit wenig Speicher und Rechenleistung ausgestatteten Edge Devices lern- und lauffähig sind.

Im Rahmen dieser Arbeit wird das Konzept „*Lifelong Deep Neural Network*“ (siehe [1]) hinsichtlich seiner Funktionalität und Anwendbarkeit auf andere Aufgabengebiete analysiert. Dazu wird eine prototypische Implementierung zur praktischen Evaluierung auf Basis der technischen Beschreibungen in [1], Behauptungen in [2] und genannten Implementierungen in [3] umgesetzt.

In Kapitel 2 werden die theoretischen Grundlagen eingeführt, in welchem zunächst auf generelle Punkte zu Deep Learning eingegangen wird. Auf Basis dieser allgemeinen Grundlagen werden detaillierter die Themen kontinuierliches und verteiltes Lernen erläutert, da diese die Hauptaspekte dieser Arbeit sind. Zudem gibt es ein Unterkapitel zu inkrementellen Klassifikatoren. In Kapitel 3 wird der L DNN A vorgestellt, mit einer anschaulichen Beschreibung und Darstellung des Ansatzes sowie einer detaillierten Erläuterung und Aufteilung des Ansatzes. Innerhalb von Kapitel 3.4 wird dieser Ansatz mit aktuellen Ansätzen des kontinuierlichen und verteilen Lernen verglichen und die Unterschiede zu gängigen Ansätzen herausgestellt. Kapitel 4 vergleicht unterschiedliche Modelle, die innerhalb des L DNN A eingesetzt werden können. Auf Basis dieser Vergleiche wird schließlich eine finale Architektur konzipiert. Der Aufbau der Evaluierung der in Kapitel 4 beschriebenen prototypischen Umsetzung des Algorithmus wird in Kapitel 5 vorgestellt. Dabei werden die verwendeten Datensätze und Metriken sowie die später durchgeführten Evaluierungsfälle vorgestellt. Die Ergebnisse sowie die Aus- und Bewertung der vorgestellten Evaluierungsfälle werden schließlich in Kapitel 6 beschrieben. Kapitel 7 beschreibt den aufgebauten Demonstrator sowie die dazu entwickelte GUI. In Kapitel 8 wird schließlich eine Zusammenfassung der Ergebnisse sowie ein Ausblick gegeben.

# Theoretische Hintergründe

In diesem Kapitel wird eine Übersicht über die theoretischen Grundlagen gegeben, welche im weiteren Verlauf der Arbeit notwendig sind. Zunächst findet eine Einführung von Deep Learning mit dem Augenmerk auf die kritischen Punkte statt. Darauf folgt eine detailliertere Einführung in die Themen kontinuierliches sowie verteiltes Lernen.

Für eine grobe Einordnung kann gesagt werden, dass Deep Learning, kontinuierliches Lernen (*Continual Learning*) und verteiltes Lernen (*Distributed Learning*) spezifische Themen aus dem Bereich des maschinellen Lernens (*Machine Learning*) sind. Abbildung 1 gibt eine graphische, beispielhafte Darstellung der Verhältnisse. Die einzelnen Bereiche haben einen hohen Überschneidungsgrad, da z.B. für das *Continual Learning* eine Vielzahl von Ansätzen des *Deep Learning* genutzt wird. Dennoch hat jeder Bereich seine eigenen spezifischen Probleme und unterschiedliche Methoden, um diese zu lösen. In dieser Arbeit werden Methoden und Komponenten aus allen Bereichen kombiniert eingesetzt und genutzt.

Abbildung 1: Verhältnis von verschiedenen Lernansätzen zu Machine Learning

## Deep Learning

In diesem Abschnitt wird eine kurze Übersicht über Deep Learning gegeben. Es wird beschrieben wie *Deep Neural Networks* (DNN) funktionieren und wie diese trainiert werden können. Zudem wird der Zusammenhang zu maschinellem Lernen aufgezeigt. Danach wird die grundlegende Struktur und das Verhalten von neuronalen Netzen erklärt sowie die Algorithmik für das Training solcher Netze eingeführt. Zum Schluss werden mögliche Probleme beim Trainieren von diesen Netzen sowie dazugehörige Lösungsansätze genannt. Es werden die grundlegenden Punkte zu Deep Learning genannt und aufgeführt, jedoch wird in dieser Arbeit nicht auf jeden Punkt detailliert eingegangen, da das Hauptaugenmerk auf der späteren Untersuchung und Bewertung des L DNN A liegt. Für detailliertere Erklärungen und Ausführung wird auf die genannten Referenzen bei den einzelnen Punkten verwiesen.

Deep Learning ist, wie in Abbildung 1 dargestellt, ein Gebiet des maschinellen Lernens. Unter maschinellem Lernen werden lernende und datenbasierte Ansätze verstanden welche eine gewisse Eingang-/Ausgangsrelation herstellen, beispielhaft dargestellt in Abbildung 2.



Abbildung 2: Generelle Problemstellung für maschinelles Lernen

Das Lernen dieser Ablaufregel geschieht mithilfe der Trainingsdaten. Dieser Zusammenhang zeigt, dass die Wahl der Trainingsdaten entscheidend ist um eine gute und generalisierte Ablaufregel zu erlernen. Machine Learning und Deep Learning Algorithmen bekommen jeweils ein gewisses Eingangssignal, welches abhängig von der Anwendung vorverarbeitet wird. Der Unterschied zwischen diesen Algorithmen ist, dass in konventionellen Machine Learning Algorithmen die Features mithilfe einer vordefinierten Regel extrahiert werden [4]. Für diese Aufgabe existiert keine Theorie und Erfahrungen von Experten sind notwendig um gute und relevante Features für die folgende Aufgabe, z.B. die Klassifikation, zu extrahieren. Die folgende Klassifikation wird von einem separaten Klassifikator durchgeführt, wie beispielsweise *kNN* (k-nearest Neighbour) oder *SVM* (Support Vector Machine). Innerhalb des Deep Learning existiert nur ein sogenanntes *Deep Neural Network* (DNN) für die Aufgaben der Feature Extraktion und Klassifikation. Das DNN lernt und adaptiert seine Netzwerkparameter mithilfe einer passenden *Loss*-Funktion. Das effiziente Anpassen der Parameter kann mithilfe des *Backpropagation*-Algorithmus umgesetzt werden ( [4], [5], [6], [7]).

Die Lernstrategie von DNNs basiert grundlegend auf der Art wie Menschen lernen zu sprechen, laufen oder rechnen. Es wird anhand von Beispielen das Verhalten soweit angepasst, bis das gewünschte Ergebnis erzielt werden kann. Obwohl Deep Learning häufig als neue Technologie gesehen wird, gab es die ersten Untersuchungen und Erscheinungen in dem Themengebiet bereits in den 1940ern. Nach Ian Goodfellow ( [4]) kann man die Geschichte des Deep Learning in drei Stufen unterteilen. Im Zeitraum von 1940 bis 1960, wo es als *Cybernetics* bekannt war. Zwischen 1980 und 1990 als *Connectionism* und das Wiederaufleben seit 2006 unter dem aktuellen Namen *Deep Learning*. Die dritte Welle der Entwicklung, in der wir uns aktuell befinden, begann mit einem Durchbruch von Geoffrey Hinton. Er konnte zeigen, dass ein spezielles neuronales Netzwerk, das sogenannte „*Deep Belief Network*“ effizient mithilfe der Strategie „*Greedy Layer-Wise Pretraining*“ trainiert werden kann [8]. Seit diesem Durchbruch stieg und steigt auch weiterhin die Anzahl der Anwendungen von DNNs deutlich an. Beispielhafte Anwendungen für DNNs heutzutage sind Empfehlungssysteme (z.B. bei Amazon), automatische Spracherkennung, Text zu Sprache Übersetzung, Objekterkennung/-klassifizierung, Bildersegmentierung und viele weitere [7]. Abhängig von der speziellen Aufgabe wird das Netzwerk und die Architektur angepasst. Aufgrund der Vielzahl an unterschiedlichen Anwendungen gibt es auch eine Vielzahl an unterschiedlichen DNN-Architekturen, beispielsweise *Convolutional Neural Networks* (CNN), *Recurrent Neural Networks* (RNN) oder *Deep Belief Nets* (DBN) [6]. Im Folgenden wird die Architektur eines DNN beispielhaft anhand eines *Feedforward Neural Network* gezeigt. Diese Netzwerke, auch als *Multilayer Perceptron* (MLP) bekannt, werden als Basis Modul innerhalb des Deep Learning bezeichnet [4]. Der Name *Feedforward* kommt von der Eigenschaft des Netzwerks, dass Information nur vorwärts (*Forward*), vom Eingangssignal durch das Netz zum Ausgangssignal, durch das Netzwerk fließt (siehe auch Abbildung 2). Diese Netzwerke besitzen keine Feedback Verbindungen. *Feedforward* Netzwerke bestehen aus mehreren Schichten (*Layer*) welche aneinandergereiht das Netzwerk bilden. Jede Schicht besteht wiederum aus mehreren Neuronen. Abbildung 3 stellt ein solches einzelnes Neuron in einem *Feedforward Neural Network* dar.



Abbildung 3: Einzelnes Neuron in einem *Feedforward Neural Network*

Diese graphische Darstellung kann auch mathematisch formuliert werden. Die mathematische Gleichung des Eingang-/Ausgangsverhaltens eines einzelnen Neurons ist in Formel **(1)** und Formel **(2)** gegeben.

|  |  |  |
| --- | --- | --- |
|  |  | (1) |

|  |  |  |
| --- | --- | --- |
|  |  | (2) |

Der Ausgang eines einzelnen Neurons wird durch die (typischerweise nicht-lineare) Aktivierungsfunktion der Aktivierung beschrieben. Die Aktivierung wiederum ist eine affine Funktion des Eingangs . Das Eingangssignal kann ein Vektor, ein zweidimensionales Bild oder ein drei- oder höherdimensionaler Tensor sein. Die trainierbaren und adaptierbaren Parameter des Neurons sind die Gewichte und der Bias .

Eine Schicht (*Layer*) des Netzwerks, dargestellt mit einzelnen Neuronen in Abbildung 4 und in komprimierter Darstellungsform in Abbildung 5, besteht allgemein aus Neuronen, welche mit dem Eingang und Ausgang verbunden sind.



Abbildung 4: Neuronen-*Layer*



Abbildung 5: Neuronen-*Layer* in komprimierter Darstellung

Neuronen in derselben Schicht sind nicht miteinanderverbunden. Abhängig von der Netzwerkarchitektur variieren die Verbindungen der Neuronen zum Ein- und Ausgang. Zwei der meist genutzten *Layer*-Architekturen sind *Dense* (auch *Fully Connected* genannt) und *Convolutional* *Layer*. Bei einem *Dense Layer* sind alle Neuronen mit jedem Eingang verbunden. Ein Netzwerk, dass nur aus solchen Schichten besteht wird F*ully Connected Network* (FCN) genannt. Der Nachteil dieser Netze sind die sehr große Anzahl an Paramatern, da jede Verbindung eine Gewichtung benötigt. Diese große Anzahl an Parametern resultiert in einer sehr hohen Komplexität bei der Berechnung und einem hohen Speicherbedarf. Zudem wird aufgrund der Verbindungen in diesen Netzwerken kein lokales Verhalten/Feature des Eingangs gelernt, da alle Neuronen voll mit dem Eingang verbunden sind und den gesamten Eingang sehen. Diese Probleme können mithilfe eines *Convolutional Neural Network* (CNN) gelöst werden. Ein CNN besteht hauptsächlich aus *convolutional Layer*. Aufgrund der Eigenschaften von diesen Schichten mit *sparsen* Verbindungen und geteilten Parametern kann der Speicherbedarf deutlich reduziert werden und das Netzwerk ist fähig, lokale Verhaltensmuster unabhängig von der Position zu erkennen. Vereinfacht gesagt fokussiert sich ein CNN auf lokale Eingangsmuster [9].

Nachdem eine Schicht definiert ist, können verschiedene Schichten zusammengeführt werden. Die resultierende Architektur stellt schließlich das Neuronale Netzwerk dar. Die finale Länge der Kette von Schichten ist die Tiefe des Modells. Von dieser Terminologie entstand der Name *Deep Learning*. Die erste und letzte Schicht wird als Eingangs- (*Input Layer*) bzw. Ausgangsschicht (*Output Layer*) bezeichnet. Diese Schichten haben definierte Größen, da der Eingang und der Ausgang des Netzwerks definierte Größen haben und damit die Dimensionen dieser Schichten bestimmen. Alle Schichten zwischen diesen beiden sind die versteckten (*hidden*) Schichten, da sie weder von der Eingangs- noch von der Ausgangsseite ersichtlich sind. Im Gegensatz zur Ein- und Ausgangsschicht ist die Größe dieser Schichten nicht fest vorgegeben und kann unabhängig von den Eingängen und Ausgängen gewählt werden. Typischerweise formen die Schichten einen Flaschenhals, welcher das Netzwerk zwingt, ein einfaches Modell des Systems zu erstellen. Dieses erlernte Modell soll in der Lage sein, generelle Muster der Daten zu erlernen um auch auf neuen, bisher unbekannten Daten (Test Daten) die gewünschte Aufgabe durchzuführen [10].

Mit nicht-lineare Aktivierungsfunktionen, wie beispielsweise Softmax (Formel **(3)**) oder *Rectifier Linear Unit* (ReLU) (Formel **(4)**), kann gezeigt werden, dass bereits ein simples MLP eine willkürliche Ein-/Ausgangs-Beziehung beliebig genau annähern kann, wenn die Anzahl von versteckten Knoten nicht begrenzt ist [10]. Diese Eigenschaft von neuronalen Netzen ist auch bekannt als Universelle Funktionsapproximation (*Universal Function Approximation*).

|  |  |  |
| --- | --- | --- |
|  |  | (3) |
|  |  | (4) |

Mit linearen Aktivierungsfunktionen ist das gesamte Netzwerk, unabhängig von der Tiefe des Netzes, nur eine lineare Transformation der Eingangsdaten. Damit können lediglich linear-lösbare Probleme gelöst werden. Das zeigt die Bedeutung von nicht-linearen Aktivierungsfunktionen.

Um ein neuronales Netzwerk mit Bezug auf das gewünschte Verhalten zu trainieren, muss eine passende Verlust- (*Loss-*) Funktion definiert werden. Diese Funktion wird auf Basis der Trainingsdaten bezüglich den Netzwerkparametern minimiert. Allgemein ist das Ziel des Trainings die Kostenfunktion auf Basis der verfügbaren Trainingsdaten zu minimieren, wie beschrieben in Formel **(5)**.

|  |  |  |
| --- | --- | --- |
|  |  | (5) |

Dabei kann eine willkürliche *Loss*-Funktion mit der gewünschten Ausgabe des Netzwerks (Label) und dem Eingang des Netzwerks für das Sample sein. Die Kostenfunktion ist der gemittelte Wert der *Loss*-Funktion über alle Trainingsdaten. Die Wahl der *Loss*-Funktion ist abhängig von der zu lösenden Problemstellung. Für Regressionsprobleme ist der l2-*Loss* eine typische Funktion, bei dem die l2 Norm des Fehlers als Optimierungskriterium genutzt wird. Der Fehler (in der Literatur *Error* genannt) ist definiert als Unterschied zwischen der gewünschten Ausgabe und der tatsächlichen Ausgabe des neuronalen Netzwerks, welcher mit der nicht-linearen Funktion beschrieben werden kann. Diese Funktion stellt den willkürlichen Zusammenhang zwischen Eingang und Ausgang dar. Der genannte l2-*Loss* ist in Gleichung **(6)** formuliert.

|  |  |  |
| --- | --- | --- |
|  |  | (6) |

Eine typische *loss*-Funktion für die Klassifikation ist der kategorische *loss*. Die Funktion ist in Gleichung **(8)** gegeben. Die letzte Schicht bei einer Klassifikationsaufgabe besitzt in der Regel eine Softmax-Aktivierungsfunktion, weshalb die finale Ausgabe des neuronalen Netzwerks () die Wahrscheinlichkeiten für die Klassenzugehörigkeit darstellt.

|  |  |  |
| --- | --- | --- |
|  |  | (7) |

Das Ziel des gesamten Trainingsprozess ist es, dass Minimum zu finden, welches im Allgemeinen keine geschlossene Lösung besitzt. Aufgrund dessen werden numerische Optimierungsverfahren im Bereich Deep Learning eingesetzt. Der meist verwendete Algorithmus zur Minimierung der Kostenfunktion ist der *Gradient Descent* (GD) Algorithmus. In diesem Algorithmus werden die Netzwerkparameter so angepasst, dass ein kleiner Schritt in Richtung des negativen Gradienten gegangen wird [5]. Der Anpassungsschritt des GD-Algorithmus kann mit Formel **(8)** beschrieben werden.

|  |  |  |
| --- | --- | --- |
|  |  | (8) |

Dabei ist der Iterationsindex und die Schrittweite (oder auch Lernrate genannt), welche die Länge des Schrittes in Richtung des negativen Gradienten Vektors bestimmt. Zu Beginn () müssen die Netzwerkparameter initialisiert werden, was eine initiale Schätzung darstellt.

Aufgrund der Größe der Trainingsdaten für neuronale Netze (z.B. 55000 Bilder für MNIST [11]) kann nicht der gesamte Datensatz im Speicher gehalten werden. Deshalb wird in der Praxis der *Stochastic Gradient Descent* (SGD) Algorithmus genutzt, welcher die Berechnungsaufwände für jede Iteration reduziert, da der Gradienten-Vektor und das Update lediglich für einen sogenannten Minibatch berechnet werden. Der stochastische Gradienten-Vektor ist die Schätzung des Gradienten-Vektors . Diese Schätzung führt zu einem verzerrten Gradienten, was wiederum zu dem Namen **stochastischer** GD führt [7].

Die Berechnung des Gradienten-Vektors ist elementar, um die Parameter anpassen zu können. Für die Berechnung des Gradienten-Vektors müssen die partiellen Ableitungen und der Kostenfunktion nach den Netzwerkparametern und berechnet werden. Dies kann mithilfe des *Error Backpropagation* Algorithmus effizient umgesetzt werden (dieser Algorithmus wird häufig auch nur *Backpropagation* oder *Backprop* genannt). Wie der Name bereits sagt, werden dabei die Error-Vektoren durch das Netzwerk rückwärts fortgepflanzt. Dabei wird das Netzwerk rückwärts durchpropagiert, beginnend bei Ausgangsschicht . Der beispielhafte Error-Vektor der Ausgangsschicht abgleitet nach den Gewichten ist in Formel **(9)** gegeben.

|  |  |  |
| --- | --- | --- |
|  |  | (9) |

Dabei ist der Ausgang und die Aktivierung von Schicht . Die partiellen Ableitungen nach folgen denselben Gleichungen, bis auf dem Austausch von durch .

Für die restlichen Schichten kann der Error-Vektor mithilfe der Kettenregel für die Differenzierung berechnet werden. Der Error-Vektor der Schicht kann mithilfe von Gleichung **(10)** berechnet werden [9].

|  |  |  |
| --- | --- | --- |
|  |  | (10) |

In den folgenden Abbildungen wird der Vorwärtspfad, sowie der Pfad der *Backpropagation*, der Rückwärtspfad, graphisch dargestellt. Abbildung 6 stellt dabei den Vorwärtspfad dar, bei dem die einzelnen Aktivierungen der Schichten berechnet werden, welche wiederum notwendig sind, um die Error-Vektoren rückwärts durch das Netzwerk propagieren zu können.

L(θ)



Abbildung 6: Vorwärts-Pfad durch ein Netzwerk

In Abbildung 7 wird die *Backpropagation* durch das Netzwerk vereinfacht graphisch dargestellt. Dafür werden die Aktivierungen, die durch den Vorwärtspfad errechnet wurden, genutzt um die Error-Vektoren (partiellen Ableitungen) zu berechnen.



Abbildung 7: Error Backpropagation durch ein Netzwerk

Abbildung 6 und Abbildung 7 stellen somit die gegensätzlichen Pfade durch ein neuronales Netzwerk dar. Der Rückwärtspfad (Backpropagation) in Abbildung 7 wird dabei nur während des Trainings eines DNN genutzt, um die Parameter anzupassen. Der Vorwärtspfad aus Abbildung 6 ist sowohl während des Trainings als auch während der späteren Anwendung aktiv. In der Trainingsphase eines DNN folgt der Rückwärtspfad immer einem vorhergehenden Vorwärtspfad durch das Netzwerk.

*Backpropagation* durch ein Netzwerk, wie in Abbildung 7, erhält als Eingangssignal den Error-Vektor der Ausgangsschicht und gibt final den Error-Vektor des gesamten Netzwerks aus. Mit der gewonnenen Information können, wie bereits beschrieben, die Netzwerkparameter entsprechend einer gewählten numerischen Optimierungsmethode (z.B. SGD) angepasst werden.

In [5] wird der Algorithmus der *Error Backpropagation* in den folgenden vier Schritten einfach zusammengefasst:

* Gebe die Eingangsdaten in das Netzwerk ein und propagiere diese wie in Abbildung 6 vorwärts durch das Netzwerk, um alle Aktivierungen der versteckten und Ausgangs Neuronen zu berechnen
* Berechne den Error-Vektor für alle Ausgangsneuronen mithilfe Formel **(9)**
* Propagiere die Error-Vektoren rückwärts durch das Netzwerk (Formel **(10)**), um die Error-Vektoren für alle versteckten Neuronen im Netzwerk zu erhalten (siehe Abbildung 7)
* Wende eine numerische Optimierungsmethode (z.B. SGD) an, um die Netzwerkparameter anzupassen

Die genannten Schritte können beliebig häufig wiederholt werden. Wenn alle Trainingsdaten einmal durch diesen Prozess durchgegangen sind, wird in der Literatur von einer Epoche gesprochen. Das Trainieren (Optimieren) eines tiefen neuronalen Netzwerks ist eine schwierige Aufgabe und kann unter einer Vielzahl von Optimierungsproblemen leiden (z.B. lokale Minima oder *vanishing* Gradient) [9].

Wie in [7] beschrieben, bietet die Optimierung eine Möglichkeit die Kostenfunktion zu minimieren. Generell sind die Ziele der Optimierung und von Deep Learning jedoch unterschiedliche. In der reinen Optimierung ist es das Ziel das Minimum einer (Trainings-) Kosten-Funktion zu finden. Im Gegensatz dazu liegt der Fokus in Deep Learning darauf, den Generalisierung-Fehler zu minimieren, welcher der Wert der Kostenfunktion auf Basis neuer, bisher nicht gekannter, Eingangsdaten ist. Deshalb ist es während dem Training wichtig, regelmäßig Validationsdaten einzuspielen, um zu überprüfen ob es eine Überanpassung (*Overfitting*) des Netzwerks auf die Trainingsdaten gibt. Überanpassung im Kontext von Deep Learning bedeutet, dass der Error auf Basis der Trainingsdaten sehr gering ist im Vergleich zu dem Generalisierungs-/Test-Error. Es gibt wiederum einige verschiedene Methoden, um einer Überanpassung vorzubeugen, wie z.B. Dropout oder Regularisierung ( [4], [5], [6], [7]).

## Kontinuierliches Lernen

Menschen und auch Tiere haben die Fähigkeit sich kontinuierlich neues Wissen anzueignen und neue Fähigkeiten zu erlernen. Diese Fähigkeit wird in der Literatur als lebenslanges (*Lifelong*) oder kontinuierliches (C*ontinual*) Lernen bezeichnet.

In diesem Kapitel werden zunächst Schwierigkeiten beim kontinuierlichen Lernen aufgeführt. Darauffolgend werden unterschiedliche Methoden vorgestellt, welche die Probleme verringern bzw. lösen sollen. Schließlich wird der Überbegriff des kontinuierlichen Lernens in unterschiedliche konkrete Anwendungsbereiche unterteilt.

Kontinuierliches Lernen kann generell als eine besondere Form des Machine Learning gesehen werden, bei der meistens dieselben Architekturen (DNNs) wie im Bereich Deep Learning genutzt werden, jedoch aufgrund spezieller Probleme teilweise andere Algorithmen im Einsatz sind. Der entscheidende Punkt beim kontinuierlichen Lernen ist, dass durch das Erlernen neuen Wissens das alte, bereits erlernte Wissen nicht verloren geht. Dieses Vergessen durch das Hinzufügen neuen Wissens wird im Bereich des maschinellen Lernens als katastrophales Vergessen (*Catastrophic Forgetting*) bezeichnet. Im Kontext von Deep Learning kann *Catastrophic Forgetting* als das Vergessen wichtiger Parameter von einer zuvor erlernten Aufgabe beim Trainieren einer neuen Aufgabe bezeichnet werden. Dieses Verhalten soll in Echtzeit-Systemen, die eine typische Anwendung von kontinuierlichem Lernen sind, vermieden werden.

Systeme, die mit der Umgebung interagieren oder bei denen sich die Umgebungsbedingungen ändern können, benötigen für eine durchgehend korrekte Funktionsweise die Fähigkeit, neue Informationen verarbeiten zu können und daraus neue Verhaltensmuster oder Entscheidungen ableiten zu können. Für das kontinuierliche Weiterlernen von DNNs gibt es verschiedene Probleme und Ansätze zum Lösen dieser, die in diesem Kapitel beleuchtet werden.

Aktuelle DNNs, welche für viele Anwendungen genutzt werden, benutzen Gradienten-basierte Methoden (z.B. SGD, siehe Kapitel 2.1). Wenn ein DNN mit solch einer Methodik inkrementell angepasst wird, erliegen diese Netze dem Problem des katastrophalen Vergessens ( [12], [13], [14]). Das liegt daran, dass diese Gradienten-basierten Methoden die Netzwerkparameter entsprechend den aktuellen Error-Vektoren anpassen, welche lediglich von den Eingangsdaten des aktuellen Minibatches abhängig sind. Der Grund für *Catastrophic Forgetting* ist bekannt als Stabilität-Plastizität Dilemma [15]. Das Modell benötigt zunächst ausreichend Plastizität (Verformbarkeit) um neue Aufgaben zu erlernen. Große Parameteränderungen bewirken jedoch das Vergessen vorher erlernter Aufgaben. Wenn die Netzwerk-Parameter stabil gehalten werden, werden vorher erlernte Aufgaben nicht vergessen, jedoch verhindert eine zu große Stabilität das Erlernen neuer Aufgaben und verringert damit die Plastizität.

Wenn beispielsweise ein Netzwerk zunächst für eine Objektklasse „Hund“ trainiert wurde und im weiteren Verlauf nur noch Katzen trainiert werden, wird die Objektklasse „Katze“ erlernt während die bereits erlernte Klasse „Hund“ höchstwahrscheinlich verlernt wird.

Intuitiv kann als Lösung für dieses Problem gefordert werden, dass die Anpassungsregel so begrenzt wird, das zuvor erlernte Informationen erhalten bleiben, während Parameter gesucht werden, um eine neue Aufgabe zu lösen. Wie in [12] beschrieben, kann das katastrophale Vergessen bildlich im Parameterraum illustriert werden. Abbildung 8 zeigt mögliche Verläufe im Parameterraum beim Erlernen einer neuen Aufgabe B nachdem Aufgabe A erlernt wurde.



Abbildung 8: Erlernen neuer Aufgabe B und mögliche Folgen

Dabei stellt die blaue Ellipsoide einen Lösungsraum mit geringem Fehler für die Aufgabe A dar mit der erlernten und gefundenen Lösung in Punkt 1. Wenn nun Aufgabe B zusätzlich erlernt werden soll, kann es im besten Fall vorkommen, dass die Parameter so angepasst werden, dass am Ende Punkt 2\* erreicht wird. Dieser Punkt ist in der Schnittmenge zwischen und und kann somit beide Aufgaben mit geringem Fehler lösen. Wenn jedoch Punkt 2 erreicht wird, kann lediglich Aufgabe B ausreichend gelöst werden. Dies ist lediglich eine einfache Beschreibung der Thematik des *Catastrophic Forgetting*. In realen Anwendungen ist die Aufgabenstellung deutlich komplexer, wodurch es keine oder nur gering überlappenden Bereiche zwischen verschiedenen Aufgaben geben kann.

Um *Catastrophic Forgetting* zu vermeiden oder den Einfluss zu minimieren, gibt es unterschiedliche Ansätze, die genutzt werden können. Eine der ersten Ansätze von 1993 [16] sieht den Grund für das Vergessen beim Backpropagation Algorithmus. Dafür entwickelte er eine Variation des Backpropagation Algorithmus. Die Idee dahinter ist, dass nur die aktiven Neuronen während dem Training angepasst werden, die für den Fehler (Error) des gesamten Netzwerks verantwortlich sind. Dadurch soll der Einfluss auf andere, bereits erlernte Muster reduziert werden. Ein weiterer früher Ansatz zur Reduzierung des *Catastrophic Forgetting* ist die Reduzierung der internen überlappenden Verteilungen, da die Überlappung der einzelnen internen Verteilung für verschiedene Muster als Grund für das *Catastrophic Forgetting* gesehen wurden [12]. Als Lösung dafür werden Semi-Distributed Repräsentation eingeführt. Die Reduzierung der repräsentativen Überlappung wird durch die Einführung von *sparsen* Vektoren erzielt. *Sparse* Vektoren bedeuten, dass nur einige wenige Neuronen aktiv sind für die Repräsentation eines speziellen Musters, was automatisch die Überlappung zu anderen Mustern reduziert. Für diese Methode wurde ein Extraschritt im normalen Backpropagation Algorithmus eingeführt, bei dem die Aktivierungsmuster für die verdeckten Schichten „geschärft“ werden. Dabei werden die Aktivierungen der Neuronen, welche am aktivsten sind, erhöht, während gleichzeitig die Aktivierungen der weniger aktiven Neuronen reduziert werden. Diese Methode konnte *Catastrophic Forgetting* signifikant reduzieren, so lange nicht zu viele Muster gelernt werden müssen.

Aus diesen frühen Ansätzen wird bereits deutlich, dass die Lernalgorithmen einen großen Einfluss auf die Eigenschaft des Vergessens haben, weshalb diese besonders im Fokus der unterschiedlichen Ansätze stehen. Nach [17] kann zwischen fünf unterschiedlichen grundlegenden Methoden zur Vermeidung des C*atastrophic Forgetting* unterschieden werden. Diese fünf Ansätze werden im Folgenden kurz vorgestellt.

Regularisierungsmethoden

Regularisierungsmethoden fügen Beschränkungen zu den Parameterupdates hinzu. Beispielhaft ist eine -Regularisierung, bei der alle Gewichte dieselbe Regularisierung erfahren, in dem Fall durch die -Norm der Gewichte. Die bekannteste und aktuell meist genutzte Methode aus dieser Kategorie ist die *Elastic Weight Consolidation* (EWC) [18]. Es wird eine Bedingung zur der *Loss*-Funktion hinzugefügt, welche Verformbarkeit (Plastizität) von den Parametern nimmt, die am relevantesten für die zuvor gelernte Aufgabe sind. Das Verhalten des EWC-Algorithmus ist graphisch in Abbildung 9 dargestellt.

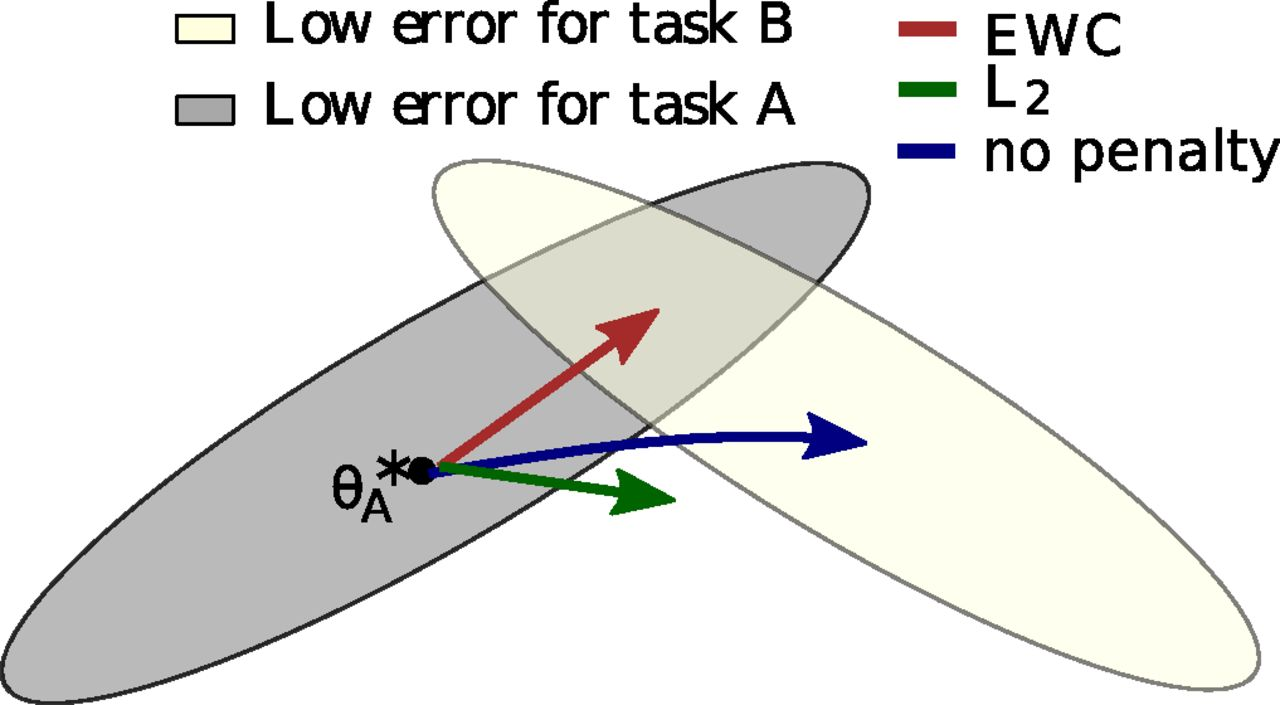


Abbildung 9: Einfluss von EWC auf Parameteranpassungen [18]

Dabei wird wieder eine einfache Darstellung des Parameterraums gewählt. Wenn keine Regularisierung gewählt wird, erzeugt das Erlernen von Aufgabe B das Verlernen der alten Aufgabe A (blauer Pfeil). Wenn alle Parameter gleich und zu stark gewichtet werden, kann die neue Aufgabe B aufgrund der geringen Anpassbarkeit der Parameter (grüner Pfeil) nicht korrekt gelernt werden. Mithilfe von EWC kann schließlich eine Lösung für die Aufgabe B gefunden werden ohne ein Vergessen von Aufgabe A (roter Pfeil). Die Funktion , welche im EWC-Algorithmus minimiert werden soll, ist in Gleichung **(11)** gegeben.

|  |  |  |
| --- | --- | --- |
|  |  | (11) |

Dabei ist die Kostenfunktion für Aufgabe B und die Gewichtung der Regularisierung. Über diese Gewichtung wird angegeben, wie wichtig die alte Aufgabe im Vergleich zur neuen ist. ist der Index der Parameter und ist die Fisher Information für jeden Parameter, welche angibt, wie relevant dieser Parameter zur Darstellung von Aufgabe A ist. sind schließlich die erlernten Parameter der Lösung für Aufgabe A, und der Startpunkt der Parameteranpassungen. Wenn eine weitere Aufgabe C hinzukommt, können die Parameter von A und B gesondert in die Formel eingehen und gewichtet werden oder die Aufgaben A und B werden als gemeinsame Aufgabe in der Gleichung gebündelt und erhalten dieselbe Gewichtung [17], [18].

Ensemble Methoden

Ensemble Methoden trainieren verschiedene Klassifikatoren und kombinieren diese unterschiedlichen Klassifikatoren um eine finale Schätzung abzugeben. Besonders frühe Ansätze dieser Methode zeigten einen klaren Nachteil bezüglich des Speicherbedarfs, da mit steigender Anzahl an Aufgaben der Speicherbedarf ansteigt. Neuere Ansätze begrenzen die Modellgröße mithilfe verschiedener Ansätze, um den Speicherbedarf zu limitieren. Der bekannteste Algorithmus dieser Methoden ist der sogenannte Pathnet-Ansatz [19]. Bei diesem Ansatz werden Agenten in einem neuronalen Netzwerk eingesetzt, welche die Teile des Netzwerks identifizieren, die für eine neue Aufgabe wiederverwendet werden können. Die relevanten Pfade für die vorherige Aufgabe werden eingefroren, um *Catstrophic Forgetting* zu vermeiden [14].

Rehearsal Methoden

Rehearsal Methoden nutzen Daten von vorhergehenden Aufgaben und fügen diese dem Trainingsprozess der neuen Aufgabe zu. Dadurch entsteht ein hoher Speicherbedarf, um die Trainingsdaten vorheriger Aufgaben zur Verfügung zu stellen. Diese Methoden wurden bereits bei frühen Ansätzen genutzt, und es lassen sich gute Ergebnisse damit erzielen. Neuere Ansätze nutzen verschiedene Methoden, um eine sinnvolle Auswahl oder Komprimierung der „alten“ Trainingsdaten zu ermöglichen, damit nur wenige relevante Daten gespeichert werden müssen. Dafür können generative Modelle wie ein Variational Autoencoder (VAE) oder Generative Adversarial Networks (GAN) genutzt werden, welche aus komprimierten Darstellungen pseudo-reale Eingangsdaten erstellen können [20], [21]. Zusammengefasst werden diese Methoden unter dem Namen *Deep Generative Replay* (DGR) [22].

Dual-Memory Methoden

Die Grundlagen für die Dual-Memory Methoden liegen in *Complementary Learning Systems* (CLS) [23]. Die CLS-Theorie baut auf den biologischen Prinzipien des Gehirnes von Säugetieren auf. In diesem werden Erinnerungen in unterschiedlichen Regionen des Gehirns abgespeichert. Frische Erinnerungen werden in einem Gebiet namens Hippocampus abgespeichert. Diese Erinnerungen werden dann langsam während des Schlafes zum Neocortex übertragen. Im Anwendungsfall ist der Neocortex für das Extrahieren von generellen Informationen zuständig, während der Hippocampus für die Erinnerung an spezifische Informationen eingesetzt wird. Eine schematische graphische Darstellung für die Dual-Memory Methode ist in Abbildung 10 zu sehen.



Abbildung 10: Schematische Darstellung der Dual-Memory Methode

Dieses Zusammenspiel eines langsam lernenden Netzes und eines schnell auffassenden Netzes wird in vielen Dual-Memory Methoden genutzt. Im Allgemeinen nutzen Dual-Memory Methoden zwei unterschiedliche Speicher und Netze, um unterschiedliche Informationen zu behalten. Die konkrete Umsetzung und Anwendung der CLS-Theorie auf die beiden zur Verfügung stehenden Netze variiert je nach Anwendungsfall und Netzwerkarchitektur [14], [17], [23].

Sparse-Coding Methoden

Bei diesen Methoden werden *sparse* Repräsentationen genutzt, welche die Wechselwirkung zwischen verschiedenen Repräsentationen (Aufgaben) reduziert. Die bereits eingeführte Methode aus [12] nutzt diese Methode, um effiziente, *sparse* Repräsentation einer Aufgabe zu erzeugen, und damit ausreichend Parameter für das Erlernen einer neuen Aufgabe verfügbar zu haben.

Nachdem verschiedene Methoden vorgestellt wurden, die das *Catastrophic Forgetting* verhindern sollen, werden nachfolgend die Anwendungen des kontinuierlichen Lernens in unterschiedliche Kategorien unterteilt, um eine sinnvolle Vergleichbarkeit und Bewertung zu ermöglichen. Nach [13] können Anwendungen des kontinuierlichen Lernens in drei Gebiete unterteilt werden: *Incremental* ***Task*** *Learning, Incremental* ***Domain*** *Learning und Incremental* ***Class*** *Learning*. Diese unterschiedlichen Szenarios werden im Folgenden definiert und der Unterschied zwischen den einzelnen Szenarios herausgestellt. Beispielhaft werden dafür zwei Aufgaben A und B angenommen, mit den Verteilungen der Eingangsdaten und , den dazugehörigen Labels und und den jeweiligen Verteilungen und . Abbildung 11 stellt die drei unterschiedlichen Szenarien am Beispiel des Split MNIST Datensatzes dar. In den gepunkteten Rechtecken wird der Eingang für das Training dargestellt, mit () für (Eingangsbild, Zielausgang, Aufgaben-ID).

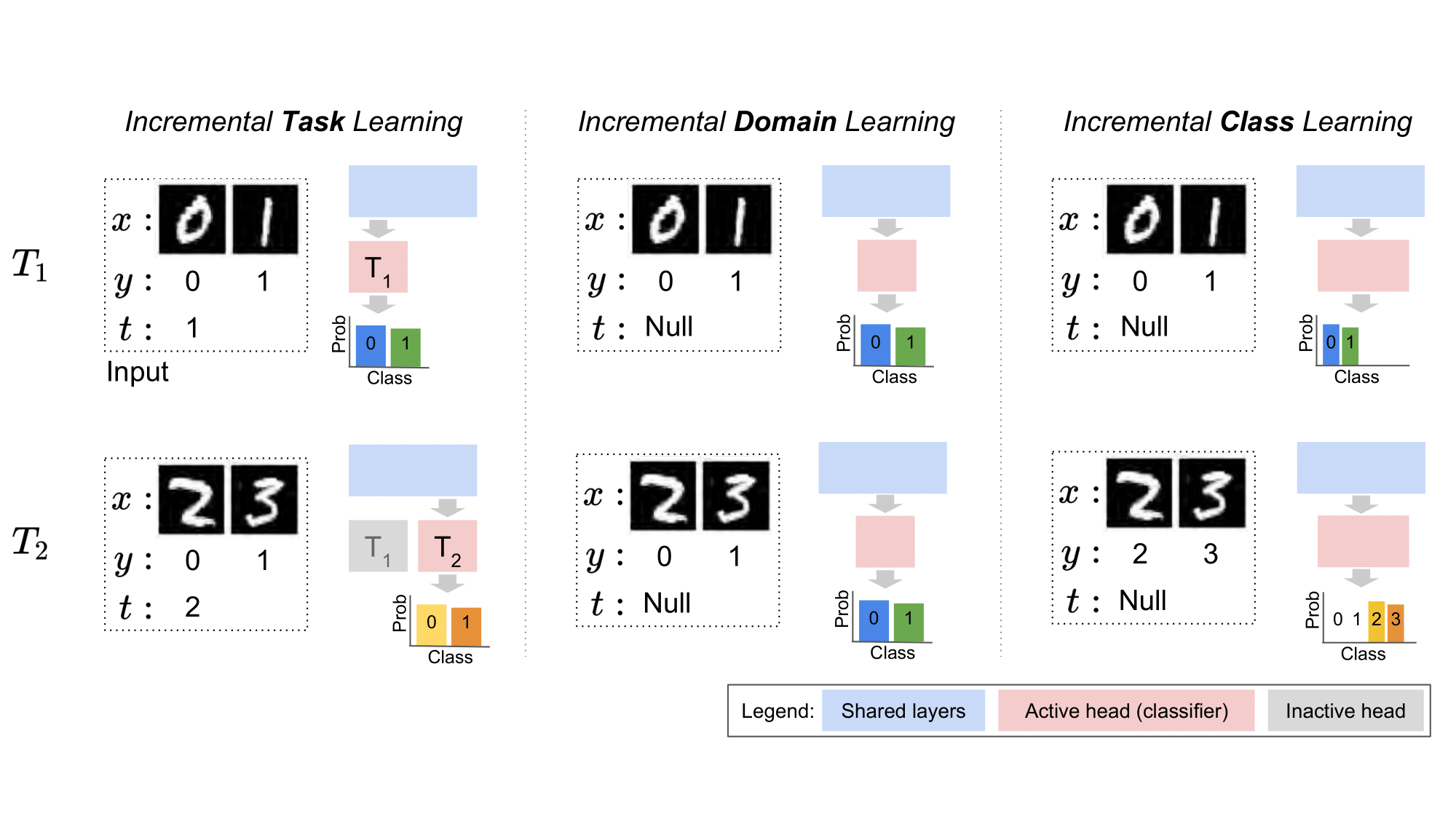


Abbildung 11: Darstellung der drei Continual Learning Szenarien am Beispiel von Split MNIST [13]

Incremental Task Learning

In diesen Szenarios haben die Aufgaben A und B unterschiedliche Ausgänge, . Daraus ergibt sich eine verschiedene Verteilung der Ausgänge, . Durch die Aufgabenstellung des kontinuierlichen Lernens gilt , da eine neue Aufgabe inkrementell erlernt werden soll. Die Ausgänge unterscheiden sich in ihrer Dimension und semantischen Bedeutung. Beispielhaft kann die erste Aufgabe eine Klassifizierung zwischen 5 Klassen sein, während die zweite Aufgabe die Regression eines einzelnen Wertes ist. Dabei wird eine komplett neue Aufgabe erlernt (z.B. Regression statt Klassifikation). Um die korrekte Ausgabe zu ermöglichen, sind aufgabenabhängige Ausgangskomponenten ( und in der linken unteren Graphik von Abbildung 11) notwendig, die abhängig von der Aufgaben-ID ausgewählt werden. Deshalb ist bei diesen Szenarien zusätzlich die Aufgaben-ID ein notwendiger Input für das Netzwerk [13].

Incremental Domain Learning

Beim inkrementellen Domain Learning variieren die Eingangsdaten, und damit . Das gesamte Netzwerk wird nicht angepasst, weshalb die Ausgabe des Netzwerks identisch bleibt mit und für ausgeglichene Datensätze auch gitl. Am Beispiel von Split MNIST mit der in Abbildung 11 dargestellten Ausgabe (binärer Klassifikator) können damit gerade von ungeraden Zahlen unterschieden werden. Bei diesen Anwendungen werden durch neue Aufgaben neue Bereiche (*Domains*) erlernt [13].

Incremental Class Learning

In diesen Szenarien werden inkrementell neue Klassen erlernt. Aufgrund der Vielzahl an Klassen gilt und aufgrund der grundlegenden Eigenschaften neuer Aufgaben auch . In diesem Aufbau wird angenommen unter der Bedingung, dass die gesamte Anzahl an Klassen bekannt ist und zu Beginn die Dimension der Ausgabe auf die gesamte Anzahl an Klassen gesetzt wird. Auch in diesem Fall behält das Netzwerk über alle Aufgaben hinweg seine Architektur und besitzt keine aufgabenabhängigen Stellen [13]. Als Variation davon kann der Anwendungsfall gesehen werden, bei dem zu Beginn nicht die finale Anzahl an Klassen bekannt ist. Dort ändert sich bei einer neuen Aufgabe (neue Klasse) der Ausgang.

Im Rahmen dieser Arbeit liegt der Fokus auf der Aufgabe des *Incremental Class Learning*. Beispielhafte Anwendung ist ein Netzwerk, das zunächst auf gewisse Klassen eines Bilddatensatzes der Objekterkennung, z.B. Hunde und Katzen, trainiert wird. Zukünftig kommen nun Vögel hinzu, welche ebenfalls klassifiziert werden sollen. Dabei bleibt die Netzwerkstruktur erhalten und es soll für jede Klasse ein eindeutig identifizierbarer Ausgang vorhanden sein.

Mithilfe der in diesem Abschnitt definierten und unterteilten Methoden sowie Aufgabengebiete lassen sich unterschiedliche kontinuierliche Lernansätze miteinander vergleichen. Zudem wurde ein grundlegendes Verständnis über Schwierigkeiten sowie Lösungsansätze für *Lifelong/Continual* lernende Algorithmen vorgestellt.

## Inkrementelle Klassifikatoren

Der untersuchte Anwendungsfall in dieser Arbeit liegt im Bereich des inkrementellen Klassen Lernens (*Incremental Class Learning*, siehe vorheriges Kapitel 2.2). Für diese Aufgabe ist es notwendig, einen inkrementellen Klassifikator einzusetzen. Generell sind inkrementelle Klassifikatoren ein spezifischer Bereich des kontinuierlichen Lernens für den konkreten Anwendungsfall der Klassifikation. Deshalb gelten auch hier die grundlegenden Probleme, welche in Kapitel 2.2 diskutiert wurden. In diesem Kapitel werden konkrete Beispiele für inkrementelle Klassifikatoren eingeführt, die später in der Konzeptionsphase verglichen und für den Anwendungsfall bewertet werden. Ein Klassifikator soll nach [24] folgende drei Punkte erfüllen, um inkrementell Klassen erlernen zu können:

* Er soll auf Basis eines Daten-Stream, in dem Sample der unterschiedlichen Klassen zu unterschiedlichen Zeitpunkten (zufällig) auftreten, trainierbar sein
* Zu jedem Zeitpunkt muss ein funktionierender Multi-Klassen Klassifikator für die bereits gesehenen und damit bekannten Klassen verfügbar sein
* Die Berechnungsanforderungen und der Speicherbedarf sollen beschränkt sein oder nur langsam ansteigen mit Bezug auf die Anzahl an bekannten Klassen

Im Folgenden werden nun beispielhaft zwei solcher inkrementellen Klassifikatoren vorgestellt:

Incremental Classifier and Representation Learning (iCaRL)

Der Incremental Classifier and Representation Learning (iCaRL) Algorithmus [24] besteht aus drei Komponenten. Die Klassifikation findet auf Basis einer *Nearest-Mean-of-Exemplars* Regel statt. Zudem gibt es eine priorisierte Exemplar-Auswahl und *Representation Learning* mithilfe von Wissens-Destillierung und prototypischen Samples. Bei diesem Algorithmus werden Klassen-Prototypen/-Repräsentationen für die unterschiedlichen Klassen angelegt. Auf Basis dieser exemplarischen Repräsentationen wird dann für ein neues Sample der Abstand zu den Repräsentationen (*Mean-of-Exemplars*) ermittelt. Schließlich folgt ein einfacher *Nearest-Mean* Klassifikator, beschrieben in Formel **(12)**.

|  |  |  |
| --- | --- | --- |
|  |  | (12) |

Dabei ist das prädizierte Label eines Inputs auf Basis der Feature-Extraktion . Der Prototypen-Vektor für jede bisher bekannte Klasse ist durch Gleichung **(13)** definiert.

|  |  |  |
| --- | --- | --- |
|  |  | (13) |

Dabei sind die Prototypen der einzelnen Klassen, definiert in der Menge . Die Anzahl an relevanten Prototypen kann dabei beliebig gewählt werden. Durch die direkte Verknüpfung der Feature-Extraktion in die Berechnung der exemplarischen Repräsentation ist sichergestellt, dass sich bei ändernder Feature-Extraktionsregel auch die Repräsentationen ändern und somit immer noch eine korrekte Klassifizierung der Eingangsdaten erfolgen kann.

Neue Daten, die für eine Klasse vorhanden sind, werden in die Berechnung der Klassenrepräsentation mit einbezogen. Dadurch kann eine kontinuierliche Weiterentwicklung und Verbesserung der Generalisierung des Klassifikators erreicht werden.

Wenn Daten für neue Klassen zur Verfügung stehen, wird mithilfe des iCaRL-Algorithmus nicht nur das exemplarische Prototypen-Set, sondern auch die Feature-Extraktion angepasst. Dafür werden die neuen Daten und die Repräsentationen der alten, bekannten Klassen als neuer Trainingsdatensatz genutzt. Nun findet ein Training nach typischen Deep Learning Algorithmen (z.B. Backpropagation) statt. Dabei soll für die neuen Daten das korrekte neue Klassenlabel ausgegeben werden, während die alten Klassen weiterhin richtig klassifiziert werden sollen. Dieser Schritt wird *Representation Learning* genannt, da auch der Feature-Extraktor und damit die Repräsentation der Eingangsdaten im Netzwerk angepasst wird. Der Algorithmus kann auch ohne *Representation Learning* genutzt werden. Es werden dann nur die Prototypen-Vektoren angepasst beziehungsweise neue Vektoren hinzugefügt, wenn neue Klassen hinzukommen.

Mit diesem Ansatz werden auf Datensätze wie ImageNet gute Ergebnisse erzielt [24]. Grundlegend baut dieser Algorithmus auf dem Prinzip des *Rehearsal Replay* auf, da die gemittelten Prototypen-Vektor für das *Representation Learning* wieder in das System eingespeist werden.

Adaptive Resonance Theory (ART)

Die Adaptive Resonanz Theorie (ART) wurde auf Basis von unterschiedlichen Aspekten, wie das Gehirn Informationen verarbeitet, entwickelt. Die ART ist nicht ein konkretes, einzelnes Modell eines neuronalen Netzwerks, sondern es beschreibt eine Familie von unterschiedlichen Modellen. Das Ziel dieser Modelle ist es, die menschliche kognitive Informations-Verarbeitung nachzubilden [25], [26]. Der große Vorteil von ART-Netzwerken ist die Fähigkeit, das Stabilitäts-Plastizitäts-Dilemma [15] zu lösen. Mithilfe von ART-Netzwerken können neue Assoziationen erlernt werden, ohne bereits bekannte Assoziationen zu verlernen. Dadurch werden diese Netzwerke häufig als inkrementelle Klassifikatoren eingesetzt werden.

Die grundlegende Intuition hinter ART Modellen ist die Idee, dass Aufgaben wie Objekt-Klassifizierung/-Erkennung beim Menschen typischerweise als Ergebnis der Interaktion von „*Top-Down*“ Erwartungen zu „*Bottom-Up*“ Eingangsdaten ablaufen. Dieses Verhalten wird auch als *Match-Based Learning* beschrieben [25]. Bei diesem Verfahren wird ein externer Input (z.B. das Bild von einer Kamera) mit internen Erinnerungen/Erwartung eines aktiven Codes verglichen. Wenn beispielsweise ein Hund von einem Menschen gesehen wird, wird das Objekt mit den bekannten Repräsentationen eines Hundes verglichen. Wenn das Objekt den Erwartungen eines Hundes erfüllt, wird das Objekt von einem Menschen als Hund erkannt.

Für ART-Modelle führt das zu dem im Folgenden erläuterten Lernalgorithmus:

Zu Beginn hat das neuronale Netz eine gewisse Anzahl an frei verfügbaren Neuronen. Die freien Neuronen dienen in einem ART-Netzwerk als Knoten für die spätere Klassifikation der Eingangsdaten. Solange keine Eingangsdaten vorliegen, befindet sich das neuronale Netzwerk in einem passiven Zustand. Wenn Eingangsdaten eintreffen, werden diese mit bisher bekannten Mustern verglichen (*gematched*). Wenn das Ergebnis des sogenannten Matching zwischen den Eingangsdaten und den bekannten Repräsentationen einen Schwellwert übersteigt, werden diese Eingangsdaten der Klasse der Repräsentation zugeordnet. Das eingehende Muster ist somit bereits bekannt. Der Schwellwert wird in einem ART-Netzwerk als *Vigilance Parameter* bezeichnet. Nachdem die Eingangsdaten einer Klasse zugeordnet werden kann, kann entweder die Netzwerkrepräsentation dieser Klasse weiter angepasst werden oder die Repräsentation wird nicht verändert. Das ist relevant, wenn eine neue Klasse auf Basis von wenigen Samples erlernt wurde. Diese Klasse kann auch nach der „Repräsentation“ im Netzwerk weiter inkrementell trainiert und damit verbessert werden. Falls der Schwellwert nicht erreicht wurde, wird ein neuer Knoten (eine neue Repräsentation) im Netzwerk erstellt und mit den Eingangsdaten initialisiert. Durch dieses Verhalten können neue Klassen erkannt und erlernt werden. Falls keine freien Knoten/Neuronen mehr verfügbar sind, können lediglich bestehende Knoten angepasst werden. Dadurch ist das Netzwerk nicht mehr in der Lage neue Klassen zu erlernen. Das muss bei der Architektur eines ART-Netzwerk berücksichtigt werden [25], [26].

Eine graphische Darstellung des beschriebenen Ablaufs ist in Abbildung 12 gegeben.



Abbildung : Ablaufdiagramm des Betriebs eines ART-Netzwerk

Zum Trainieren eines ART-Netzwerks gibt es zwei unterschiedliche Methoden, das langsame und das schnelle Training/Lernen. Das langsame Training ähnelt dabei mehr dem biologischen Prozess und nutzt Differenzialgleichungen zur kontinuierlichen und iterativen, aber langsamen Anpassung der Gewichte. Dies wird typischerweise bei kontinuierlichen Datenströmen eingesetzt, da dort die Eingangsdaten über einen längeren Zeitraum anliegen, und somit das System die Möglichkeit hat sich langsam an den gewünschten Grenzwert anzupassen. Das schnelle Lernen (*Fast Learning*) ermöglicht dem System sich schnell auf seltene Eingangsdaten anzupassen. Dabei werden die Netzwerkparameter auf die berechneten asymptotischen Parameterwerte gesetzt [25], [26].

Wie bereits beschrieben, gibt es unterschiedliche ART-Architekturen, die je nach Anwendungsfall variieren. Diese werden hier nicht einzeln detailliert aufgelistet.

In diesem Abschnitt wurden zwei beispielhafte inkrementelle Klassifikatoren vorgestellt und deren prinzipielle Betriebsweise erläutert. Auf Basis dieser eingeführten Klassifikatoren kann für den in dieser Arbeit relevanten Anwendungsfall ein passender inkrementeller Klassifikator ausgewählt werden.

## Verteiltes Lernen

Verteiltes Lernen wird in der Literatur unter den Namen *Distributed* oder *Parallel* *Learning* beschrieben. Es gibt viele unterschiedliche Gründe, warum verteiltes Lernen eingesetzt wird. Beispielsweise kann es aufgrund der Größe des Netzwerkes notwendig sein das Modell auf mehrere Prozessoren zu verteilen. Auch kann es wegen der langen Trainingszeiten von DNNs bei großen Datenmengen gewünscht sein, paralleles und verteiltes Training mit aufgeteilten Datensätzen durchzuführen und die verschiedenen trainierten Modelle nach dem Training (in der Literatur *post-training* genannt) zusammenzuführen. Ein anderer Anwendungsfall kann schließlich das Sammeln von riesigen Datenmengen auf lokalen verteilten Geräten (z.B. Smartphones) sein. Da nur begrenzter Speicher zur Verfügung steht und Datenschutzrichtlinien eingehalten werden müssen, können die lokal gesammelten Daten häufig nicht auf einen zentralen Server geladen werden, wo ein zentralisiertes Training stattfinden könnte. Deshalb kann es notwendig sein auf den jeweiligen Endgeräten verteilt und lokal zu trainieren (lernen) und lediglich Parameteränderungen auf einem Server zu sammeln, um am Ende ein besseres globales Netzwerk zu erhalten. Dadurch liegen sicherheitskritische Daten nicht zentral gesammelt auf einem Server, sondern verteilt auf den Endgeräten, wodurch das Sicherheitsrisiko verringert werden kann.

In diesem Kapitel werden nachfolgend unterschiedliche Anwendungsgebiete, sowie die dazugehörigen Ansätze und Methoden des verteilten und parallelen Lernens eingeführt. Aufgrund der Vielzahl an unterschiedlichen Methoden werden nur ausgewählte, im Rahmen dieser Arbeit relevante, Methoden vorgestellt.

Ursprünglich entstand der Wunsch nach verteiltem und parallelem Lernen durch die langen Trainingszeiten von komplexen neuronalen Netzwerken. Komplexe Netzwerke, die auf großen Datensätzen trainiert werden, können Tage bis Wochen auf einzelnen Prozessoren benötigen, um die Parametrisierung zu erlernen. Durch die Weiterentwicklung und Nutzung von *Graphical Processing Units* (GPUs) kann das Training von DNNs bereits deutlich beschleunigt werden. Dennoch kann durch paralleles, verteiltes Training diese Rechenzeit weiter reduziert werden. Zudem kann es auch vorkommen, dass Datensätze oder Modelle zu groß sind um auf einem einzigen Gerät gespeichert zu werden.

Zur Einordnung kann vereinfacht zwischen lokalem und verteiltem Training unterschieden werden. Bei lokalem Training werden die Daten und das Modell auf einem einzelnen Gerät gespeichert. Es können mehrere Kerne dieses Geräts zur Parallelisierung genutzt werden. Zum Beispiel können unterschiedliche Kerne genutzt werden um verschiedene Inputs parallel zu bearbeiten oder die unterschiedlichen Kerne können genutzt werden um mehrere Minibatches parallel zu prozessieren.

Beim verteilten Training ist es nicht möglich und/oder nicht erwünscht den gesamten Datensatz oder das gesamte Modell auf einem einzelnen Gerät, sondern auf mehreren Geräten verteilt zu speichern.

Für eine feinere Aufteilung wird zwischen der Parallelisierung in Netzwerken allgemein und der Parallelisierung im Training von diesen Netzwerken unterschieden werden. Für die Parallelisierung in Netzwerken kann zwischen Daten-Parallelisierung und Modell-Parallelisierung unterschieden werden.

Bei der Daten-Parallelisierung werden die Daten auf verschiedene Geräte verteilt, wenn die Datenmenge zu groß ist oder ein schnelleres Training erwünscht ist. Modell-Parallelisierung wird angewendet, wenn das Modell speichertechnisch nicht auf einem Gerät gespeichert werden kann. Dabei werden dann unterschiedliche Schichten des neuronalen Netzwerkes auf unterschiedliche Geräte verteilt werden. Dies erfordert eine Kommunikation der Geräte um die Daten durch das Netzwerk zu propagieren und auch um Backpropagation durchführen zu können [27].

In [28] wird genauer die Parallelisierung des Trainings von Netzwerken beschrieben. Im Rahmen dieser Arbeit sind besonders diese Methoden und Ansätze interessant, weshalb auf diese nun detaillierter eingegangen wird. In den bisher eingeführten Parallelisierungen/Verteilungen der Modelle oder Daten existiert lediglich eine Version der Parameter des Netzes. In den nachfolgenden Methoden existiert generell mehr als eine Instanz der Netzwerk-Parameter. Die Ansätze können dabei in drei Kategorien unterteilt werden: Modell-Übereinstimmung, Parameter-Verteilung und Training-Verteilung. Zu jeder Kategorie gibt es verschiedene Methoden, von denen einige beispielhaft in Tabelle 1 zusammengefasst werden [28].

Tabelle 1: Übersicht über Verteilte Deep Learning Methoden

|  |  |
| --- | --- |
| Kategorie | Methode |
| Model-Übereinstimmung | |
| *Synchronisation* | Synchron  Asynchron  Nicht-deterministische Kommunikation |
| Parameter-Verteilung und Kommunikation | |
| *Zentralisierung* | Parameter Server (PS)  Dezentralisiert |
| Training-Verteilung | |
| *Modell-Konsolidierung* | Ensemble Lernen  Wissens-Destillierung |

Nachfolgend wird auf einzelne Methoden spezifischer eingegangen, wobei in einer späteren Anwendung die unterschiedlichen Methoden miteinander genutzt werden können, da sie unterschiedliche Aspekte des verteilten Lernens behandeln:

Modell-Übereinstimmung

In den Methoden, welche in der Kategorie Modell-Übereinstimmung zusammengefasst sind, werden Berechnungen der Update-Schritte parallel auf unterschiedlichen Knoten ausgeführt. Diese Methoden können als eine spezielle Form der Daten-Parallelisierung angesehen werden. Aktuelle Parameter auf einem *Master-*Gerät werden als konsistentes Modell angesehen. Das Master-Gerät kann dabei durch einen zentralen Parameter Server (PS) oder dezentralisiert auf unterschiedlichen Knoten realisiert werden. Bei synchronen Methoden senden alle Knoten zum gleichen Zeitpunkt ihre entsprechend berechneten Parameteränderungen, welche zentral zu einem neuen konsistenten Modell zusammengefasst werden. Dieses Modell wird wieder verteilt und die unterschiedlichen Knoten können den nächsten Zyklus (Minibatch) durchführen. Bei asynchronen Methoden findet diese Synchronisation asynchron zu unterschiedlichen Zeitpunkten statt. Bei einer nicht-deterministischen Kommunikation kann beispielsweise event-getriggert die Synchronisation stattfinden, z.B. nach einer gewissen Anzahl an Trainingsschritten [27], [28].

Parameter-Verteilung und Kommunikation

Eine zentralisierte Netzwerkarchitektur beinhaltet in der Regel eine PS-Infrastruktur. Mit dieser Infrastruktur senden die einzelnen Knoten ihre Änderungen, was im Fall eines DNN der errechnete Gradient ist, zu einem zentralen PS. Die eintreffenden Gradienten werden von dem zentralen PS benutzt, um neue Parameterwerte zu berechnen. Es gibt in diesem Szenario somit nur einen zentralen Optimierer. Die neu optimierten Parameter werden als Antwort an die unterschiedlichen Knoten verteilt. Bei einem dezentralisierten Ansatz besitzt jeder Knoten einen eigenen Optimierer wodurch jeder Knoten separate Parameteranpassungen berechnet und durchführt. Die unterschiedlichen Knoten können untereinander kommunizieren und Parameter austauschen.

Generell ist eine PS Infrastruktur für die Leistung und die Fehlertoleranz des Netzwerkes förderlich, da mithilfe eines zentralisierten PS Checkpoints zentral gespeichert werden können. Bei Erkennen eines möglichen Overfittings oder anderen unterwünschten Trainingseffekten kann auf einen zuvor gespeicherten Checkpoint zurückgegangen werden. Dennoch müssen bei diesem Ansatz auch die Kommunikationskosten abgewogen werden, die durch einen zentralen PS im Vergleich zu einem dezentralisierten Ansatz entstehen [27], [28].

Training-Verteilung

In diesen Ansätzen finden nur selten und unregelmäßig Parameterupdates, beziehungsweise der Austausch von Parametern, statt. Es werden auf unterschiedlichen Knoten Kopien der Parameter angelegt und die durch das Training erhaltenen Parameter nach dem Training (*Post-Training*) oder einige Male während dem Training kombiniert. Eine bekannte und häufig genutzte Kombinationsmöglichkeit nach dem Training ist das Ensemble Lernen. Beim Ensemble Lernen werden mehrere Instanzen des Netzwerks angelegt und parallel und unabhängig voneinander trainiert. Es findet keine Kommunikation zwischen den einzelnen Knoten während des Trainings statt. Die finale Ausgabe des Ensembles ist die kombinierte Ausgabe der einzelnen Netzwerke. Die Gewichtung kann dabei gleichmäßig geschehen, was dem Mittelwert der unterschiedlichen Netzwerkausgänge entspricht. Alternativ können die Ausgänge einzelner Netzwerke, welche als vertrauenswürdiger eingestuft werden, stärker gewichtet werden. Eine weitere *Post-Training* Methode ist die Wissens-Destillierung (*Knowledge-Distillation*). Bei dieser Methode wird die Größe des DNNs reduziert indem ein zweistufiges Training stattfindet. Zunächst wird ein großes Netzwerk oder ein Ensemble von mehreren Netzwerken trainiert. Im zweiten Schritt wird ein neuronales Netzwerk trainiert, das den Ausgang des großen Ensembles imitiert. Mit diesen kleineren Netzwerken können dieselben Ergebnisse wie mit größeren Ensembles erzielt werden [28].

Als zusätzliche, spezifische Methode wird verbündetes Lernen (*federated* Learning) vorgestellt. Diese Methode wurde 2016 in [29] vorgestellt. Das Ziel dieser Methode ist ein hochqualitatives, zentralisiertes Modell auf Basis vieler verteilter Netzwerke zu trainieren. Dabei liegen die Daten ungleichmäßig verteilt über diese Knoten vor. Die lokalen Knoten werden dabei als Rechnerknoten benutzt, die mithilfe der lokalen Daten Optimierungen durchführen. Die lokalen Daten müssen bei dieser Methode nicht auf einem zentralen Server gespeichert werden, sondern liegen nur auf den lokalen Knoten vor. Mithilfe dieses Aufbaus müssen mögliche private, sicherheitskritische Daten nicht auf einen Server geladen werden, was die Reduzierung des Sicherheitsrisikos zur Folge hat. Zudem kann mit dieser Methode der Kommunikationsaufwand zwischen den einzelnen Knoten und einem zentralen Server (globales Modell) sowie die Kommunikation unter den Knoten minimiert werden. In dem Ansatz des verbündeten Lernens werden lediglich Anpassungen an den zentralen Server geschickt (z.B. Gradienten-Vektor), wodurch die benötigte Kommunikationsbandbreite im Vergleich zu den kompletten Trainingsdaten drastisch reduziert wird. Gleichzeitig ist die geschickte Information deutlich abstrahierter von den möglicherweise personalisierten Daten. *Federated Learning* kann mit folgenden Notationen definiert werden: Es gibt Besitzer von Knoten (z.B. Smartphones), mit den gesammelten persönlichen Daten . In klassischen Ansätzen würden die Daten zusammengelegt mit um ein zentrales Modell zu trainieren. Ein föderiertes System ist ein lernender Prozess, in dem die einzelnen Knoten jeweils ein eigenes Modell trainieren. Dabei werden die Daten der einzelnen Knoten nicht mit den anderen Knoten geteilt. Zusätzlich soll die Genauigkeit der einzelnen Modelle, beschrieben durch , annähernd die Genauigkeit des hypothetischen zentralen Modells , , erreichen. Mathematisch kann das mithilfe der nicht-negativen realen Zahl in Gleichung **(14)** beschrieben werden:

|  |  |  |
| --- | --- | --- |
|  |  | (14) |

Ein föderiertes System hat somit einen -Genauigkeit Verlust. Föderierte Systeme können weiter in unterschiedliche Anwendungsfälle kategorisiert werden, die in Tabelle 2 dargestellt werden [30].

Tabelle 2: Kategorisierung von *Federated Learning*

|  |  |
| --- | --- |
| Kategorie | Beschreibung |
| Horizontales Federated Learning | Unterschiedliche Samples, Gleiche Features |
| Vertikales Federated Learning | Gleiche Samples, Unterschiedliche Features |

Für ein besseres Verständnis werden konkrete Beispiele für die unterschiedlichen Kategorien gegeben:

Horizontales Federated Learning

Zwei regionale Banken mit unterschiedlichen Benutzergruppen aus ihren jeweiligen Regionen haben eine geringe (keine) Überschneidung der Kunden. Das Geschäft der beiden Banken ist jedoch sehr ähnlich, wodurch die Features sehr ähnlich sind. Für eine bessere Generalisierung können die Parameter der unabhängig trainierten Netze nach dem Training ausgetauscht werden.

Vertikales Federated Learning

Zwei unterschiedliche Firmen in der gleichen Stadt, eine Bank und ein Internetshop, haben eine sehr große Überschneidung bei den Nutzern. Die Features der beiden Firmen sind jedoch sehr unterschiedlich. Die Bank speichert zum Beispiel das monatlich einkommende Gehalt und das Kreditranking, während der Internetshop Browserverläufe und Einkaufsverhalten abspeichert. Durch das Verbünden beider auf Basis der Features trainierten Netzwerke kann mithilfe der Kundendaten das Einkaufsverhalten einzelner Gruppen/Personen genauer vorhergesagt werden

Im Rahmen dieser Arbeit ist das horizontale *Federated Learning* der relevante Anwendungsfall. Der prototypische Anwendungsfall in dieser Arbeit für das verteilte Lernen ist die Objekterkennung in Bildern. Die verschiedenen Bilder haben dieselben grundlegen Features wie z.B. Kanten, Farbe oder Form der Objekte. Jedoch sehen unterschiedliche Netzwerke unterschiedliche Bilder bei diesem Anwendungsbeispiel des verteilten Lernens. Beispielsweise sieht Netzwerk A nur Bilder von Hunden und Katzen während des Trainings. Netzwerk B sieht dafür Kamele und Frösche. Nach dem Training sollen, durch den Austausch von Parametern der föderierten Netzwerke, beide Netzwerke in der Lage sein, alle vier Tiere klassifizieren zu können.

In diesem Abschnitt wurden unterschiedliche Gründe und Anwendungsgebiete für den Einsatz von verteiltem Lernen dargestellt. Zudem wurden Schwierigkeiten und unterschiedliche Methoden dargestellt. Die unterschiedlichen Methoden wurden in Kategorien eingeteilt. Zum Ende wurde ein aktueller spezifischer Algorithmus des verteilten Lernens beschrieben, der für den im Rahmen dieser Arbeit untersuchten Anwendungsfall mögliche Lösungen bereithält.

# Lifelong Deep Neural Network Algorithmus

In dieser Arbeit wird ein Lifelong Deep Neural Network Algorithmus untersucht und prototypisch umgesetzt. Der Algorithmus ist in [1] detailliert beschrieben. In diesem Kapitel wird der Algorithmus, sowie Vor- und Nachteile davon beschrieben. Auch werden Behauptungen, die nach [2] durch den Algorithmus möglich sind, genannt und auch in Relation zu bereits bekannten Methoden gesetzt. Zum Schluss wird eine kurze Zusammenfassung gegeben.

## Beschreibung

Der Lifelong Deep Neural Network Algorithmus soll den Bereich von Deep Learning revolutionieren, indem er schnelles Lernen nach Auslieferung ohne ausführliches Training, vielen Rechenressourcen oder extremer Datenspeicherung ermöglicht [1]. Dafür wurden mehrere Punkte gefunden, die bei bisherigen Deep Learning Ansätzen (welche den Backpropagation Algorithmus nutzen) ein Problem darstellen, um die oben genannten Punkte zu erfüllen. Nach [1] können die Probleme in den folgenden fünf Punkten zusammengefasst werden, welche den bisherigen Einsatz von Deep Learning Algorithmen eingrenzen:

* Es ist unmöglich das System „on-the-fly“ mit neuem Wissen upzudaten
* Lernen während dem gesamten Einsatzzyklus eines Gerätes ist ohne regelmäßige Kommunikation mit Servern und ohne eine erhebliche Wartezeit für ein Wissensupdate unmöglich
* Das Erlernen neuer Informationen verbraucht Serverspeicher, Energie und lokalen Gerätespeicher um alle Eingangsdaten unendlich lange für das weitere Training abzuspeichern
* Es ist unmöglich auf einem kleinen Endgerät zu lernen (trainieren)
* Es ist nicht möglich Wissen über mehrere Endgeräte auszutauschen ohne ein langsames und teures Training auf einem Server und Neuverteilung der erlernten Parameter

Diese beschriebenen Probleme sind bekannte Probleme des Deep Learnings, und wurden bereits in den vorhergehenden Kapiteln teilweise beschrieben.

In diesem Lifelong Deep Neural Network Algorithmus sollen nun mithilfe von zwei Modulen diese Probleme überwunden werden. Dafür wird ein langsam lernendes neuronales Netzwerk (z.B. DNN) als erste Stufe genutzt (Modul A). Dieses Netzwerk ist ein vortrainierter Feature-Extraktor. Je nach Anwendungsfall kann dieses Netzwerk theoretisch während der Laufzeit weiter trainiert werden mit kleinen, langsamen Updateschritten oder es wird nach dem Vortraining fixiert. Modul A wird mithilfe des Backpropagation-Algorithmus auf Basis von repräsentativen Datensätzen vortrainiert. Ein beispielhafter Datensatz, der für das Vortrainieren solche Feature-Extraktoren für Bilderklassifizierung genutzt wird, ist ImageNet [31]. Dieser Datensatz besitzt mit 1000 verschiedenen Klassen eine sehr große Varianz der Objekte, wodurch eine gute Generalisierbarkeit erreicht werden kann.

Von dem vortrainierten DNN wird eine der letzten Feature-Schichten als Eingang des zweiten Moduls, Modul B, genutzt. Typischerweise wird als Interface die letzte Schicht des DNN vor der DNN-eigenen Klassifikationsschicht genutzt. Abbildung 13 zeigt ein beispielhaftes Modul A sowie das Interface zu Modul B. Jedes Rechteck stellt dabei eine willkürliche (Convolutional, Fully Connected) Schicht eines DNN dar. Die letzte grüne Schicht stellt die Schicht dar, welche für die Klassifikation verantwortlich ist. Innerhalb des L DNN Algorithmus wird diese Schicht nicht genutzt, sondern die Features der Schicht davor werden als Eingang für Modul B genutzt. Somit stellt Modul A eine modifizierte Version des vortrainierten DNN dar.



Abbildung 13: Modul A und Interface zu Modul B

Modul B ist ein inkrementeller Klassifikator, der Gewichte und Repräsentationen auf Basis von wenigen Trainingsdaten ändern kann. Modul B erhält die extrahierten Features von Modul A und kann mithilfe dieser z.B. die Klassifikation durchführen. Falls die erhaltenen Repräsentationen nicht bekannt sind, bzw. zu keiner bekannten Klasse passen, kann Modul B durch Interaktion mit dem User das korrekte Label erhalten und aufgrund seiner schnell lernenden Eigenschaft diese neue Klasse mit wenigen Samples erlernen. In [1] genannte Beispiele für ein Modul B sind z.B. ein *Adaptive Resonance Theory* (ART) Netzwerk oder als nicht-neuronale Methode die *Support Vector Machine* (SVM). Generell kann jeder schnell lernende, überwachte Klassifikator-Prozess genutzt werden.

Die grundsätzliche, allgemeine Architektur des L DNN Algorithmus ist in Abbildung 14 dargestellt.



Abbildung 14: Graphische Darstellung des L DNN A

Je nach Anwendungsfall variieren die Eingangsdaten und die Ausgabe. Die konkreten Module A und B können nach Bedarf gewählt und geändert werden.

Der Algorithmus ist so aufgebaut, dass auf mehreren Geräten parallel neues Wissen erlernt werden kann. Dieses Wissen kann durch den direkten Austausch einzelner Geräte oder durch eine zentrale Steuerung über einen Server ausgetauscht werden. Dafür können beliebig viele parallele Geräte, die mit einem L DNN Algorithmus ausgestattet sind, verbunden werden. Ein beispielhaftes Szenario ist in Abbildung 15 dargestellt. In diesem Szenario sind einzelne Geräte (in der Graphik die beiden linken Geräte) direkt miteinander verbunden. Zusätzlich gibt es einen zentralen Server, der mit allen Geräten verbunden ist und von diesen Updates erhält. Dieser zentrale Server kann wiederum dann kombinierte Parameterupdates verteilen.



Abbildung 15: Beispielhaftes Szenario mit mehreren Endgeräten und einem zentralen Server

Wie zu sehen ist, tauschen sich die schnell lernenden Module B aus, da dort das sich ändernde Netzwerk implementiert ist. So können Objektklassen, die von einem Gerät gesehen und erlernt werden mit anderen Geräten geteilt werden. Dadurch erhalten die anderen Geräte ebenfalls die Fähigkeit, diese neue Objektklasse bestimmen zu können, ohne jemals ein Objekt dieser Klasse gesehen zu haben.

Der Aufteilung in Kapitel 2 folgend ist es bei diesem Algorithmus sinnvoll, zwei Themen separat zu behandeln. Die Fähigkeit und Methoden des kontinuierlichen Lernens und des verteilten Lernens. Diese beiden Themen werden mit Bezug auf den beschriebenen Algorithmus im Folgenden detaillierter untersucht.

### Kontinuierliches Lernen

Der grundlegende Aufbau des L DNN Algorithmus hinsichtlich kontinuierlichen Lernens basiert auf der Dual-Memory Methode. Es werden zwei Submodule genutzt. Ein langsam lernendes oder fixiertes Modul und ein schnell lernendes Modul, welches neue Informationen schnell erkennen und erlernen soll. Die grundlegende Idee dieser Architektur kommt von dem Gehirn der Säugetiere (Details in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**). Für das kontinuierliche Lernen ist hauptsächlich Modul B relevant, da Modul A als Feature-Extraktor auf Basis der Eingangsdaten fix ist oder sich nur sehr langsam ändert. Die Aufgabe, welche mit diesem Ansatz gelöst werden kann ist das inkrementelle Klassen Lernen (*Incremental Class Learning*). Das bedeutet, dass die grundlegende Aufgabe, z.B. Objekterkennung, gleich bleibt während des Lebenszyklus des Algorithmus. Es können jedoch neue Klassen erlernt werden.

Modul B ist ein schnell lernender Klassifikator, der bereits vortrainiert sein kann für manche Klassen oder komplett untrainiert während des Betriebes trainiert werden kann. Dafür ist ein Feedback des Nutzers nötig, um korrekte Labels und Klassenbezeichnungen zu erhalten. Das gewünschte Verhalten von Modul B wird im Folgenden kurz erläutert:

Wenn Feature-Vektoren von Modul A eintreffen, soll auf Basis der bereits bekannten Klassen die Klassenzugehörigkeit ermittelt werden. Wenn User-Feedback für dieses Sample vorhanden ist, soll eine weitere Anpassung für diese Klassen stattfinden, um eine bessere Generalisierbarkeit zu erreichen. Somit soll auch für bereits bekannte Klassen kontinuierlich weitergelernt werden. Für den speziellen Fall, dass die Klasse des Samples nicht bekannt ist, wird in dem L DNN Algorithmus das „*Nothing I know*“-Konzept vorgeschlagen. Dafür wird ein Schwellwert für die Klassenzugehörigkeit definiert, der erreicht werden muss, damit die Klasse dem Sample zugeordnet wird. Wenn dieser Schwellwert nicht erreicht wird, ordnet der Algorithmus dieses Sample der Klasse „*Nothing I know*“ zu. In diesem Fall wird der User aufgefordert, die Klasse des Sample zu benennen, damit die neue Klasse auf Basis des Samples erlernt werden kann (*One-Shot Learning*). In [1] wird für die Berechnung des Schwellwertes folgende Gleichung **(15)** genannt:

|  |  |  |
| --- | --- | --- |
|  |  | (15) |

Dabei stellt die Anzahl an bereits erlernten Kategorien (Klassen) dar und die gesamte Anzahl an Kategorie-Knoten im Netzwerk. Der Skalierungsfaktor wird auf Basis des genutzten DNN in Modul A angepasst und gesetzt. Wenn dieser Wert zu hoch gewählt wird, steigt die False Negative Rate, da potentiell zu häufig neue Klassen erstellt werden. Ein zu niedriger Wert von vergrößert die False Positive Rate, da Samples von neuen, bisher unbekannten Klassen potentiell zu bekannten Klassen zugeordnet werden.

Ein ausgewähltes Klassifikator-Netzwerk, welches diese Anforderungen erfüllen kann, wird dann schließlich als Modul B genutzt. Unterschiedliche Ansätze für das Modul B werden in der folgenden Konzeptionsphase beleuchtet und untersucht.

### Verteiltes Lernen

Der L DNN Algorithmus nutzt von seinem Aufbau das Prinzip der Trainings-Verteilung. Auf mehreren Endgeräten liegen jeweils unabhängige Kopien der Parameter vor, welche dort lokal angepasst werden und gegebenenfalls direkt zwischen den Geräten oder über einen zentralen Server ausgetauscht werden können (siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**). Wie in Abbildung 15 exemplarisch dargestellt, sind die unterschiedlichen Module B für den Austausch der Parameter relevant, da in diesen Modulen die Parameter während der Benutzung kontinuierlich angepasst werden. Das Grundprinzip dabei ähnelt dem Prinzip des *Federated Learning* [29],[30]. Es werden auf mehreren Geräten lokale Daten generiert, welche jedoch nur genutzt werden um das lokale Netzwerk zu trainieren. Diese geänderten und erlernten Parameter können dann wiederum ausgetauscht werden, um neues Wissen auszutauschen. Nach der Kategorisierung aus Tabelle 2 kann der hier genutzte Anwendungsfall in die Kategorie des horizontalen *Federated Learning* eingegliedert werden, da die genutzten Features von Modul B identisch sind (aufgrund desselben Moduls A), jedoch unterschiedliche Samples gesehen werden.

Der L DNN Algorithmus besitzt einen zusätzlichen Schritt, die Konsolidierung neuen Wissens. Dieser Schritt wird genutzt um eine effiziente Struktur der einzelnen Klassifikatoren zu erzielen, wodurch der Speicherbedarf gesenkt werden kann und dadurch auch der Kommunikationsaufwand für die Parameterupdates verringert werden kann. Die Konsolidierung findet statt, nachdem eine oder mehrere Objekte *on-the-fly* gelernt wurden. Dabei werden die Repräsentationen der neuen Objekte komprimiert und diese neuen Objekte mit den Repräsentationen bereits bekannter Objekte integriert. Dadurch soll die Generalisierung des Netzwerks verbessert werden und der Speicherbedarf reduziert werden.

Dieses konsolidierte Wissen der einzelnen Netzwerke kann dann kommuniziert werden. Dafür werden zu willkürlichen Zeitpunkten (z.B. nachdem neue Klassen erlernt wurden, nach einem definierten Zeitraum etc.) die konsolidierten Parameter des schnell lernenden Moduls B ausgetauscht. Dies kann geschehen, indem alle Geräte ihre Parameter einem zentralen Server/Gerät melden, oder einzelne Geräte tauschen sich „peer-to-peer“ untereinander aus. Wenn in einem zentralen Punkt (auf einem Server oder einem Mastergerät) alle Parameter zusammentreffen, kann die Fusion der einzelnen erlernten Parameter stattfinden. Beim Kombinieren der Parameter werden Redundanzen zwischen einzelnen Geräten entfernt und der Speicherbedarf wird durch das Kombinieren mehrerer Parameter gesenkt im Vergleich zu einem naiven Ansatz, bei dem alle Repräsentationen aneinandergehängt werden. Zudem kann dabei die Generalisierung weiter verbessert werden, da Einflüsse von unterschiedlichen Daten die Parameter der einzelnen Geräte beeinflusst haben. Weiterhin soll die Genauigkeit des Systems erhalten werden und durch das Kombinieren im besten Fall weiter verbessert werden. Diese kombinierten Parameter können wiederum als Parameterupdates an alle Geräte versendet werden. Alternativ kann auch das zentrale Netzwerk für weitere Anwendungen genutzt werden. Durch das Verteilen der kombinierten Parameter kann das erlernte Wissen vieler verteilter Geräte konsolidiert werden und neues Wissen, das einzelne Geräte erlernt haben, mit anderen Geräten ausgetauscht werden.

## Vorteile

Der dargestellte Algorithmus hat nach den Behauptungen in [1] und [2] gegenüber klassischen DNN-Architekturen und Algorithmen einige Vorteile zu bieten, die im Folgend genannt und erläutert werden.

Der große beschriebene Vorteil des L DNN Algorithmus ist seine Fähigkeit, kontinuierlich zu lernen ohne dabei dem Problem des *Catastrophic Forgetting* zu unterliegen. Maßgeblich dafür entscheidend ist, dass für das schnelllernende Modul B kein Backpropagation Algorithmus genutzt wird. Dies kann durch die zweistufige Architektur erzielt werden (Dual-Memory Method). Mithilfe des Algorithmus können inkrementell neue Klassen schnell erlernt werden, ohne dafür alte Trainingsdaten zu benötigen. Dadurch ist keine Speicherung großer Datenmengen notwendig. Zudem soll es durch diese beiden Behauptungen möglich sein auf einem lokalen Endgerät (z.B. Smartphone) ohne große Rechen- oder Speicherkapazität weiter zu lernen. Aufgrund der beschriebenen Architektur sollen deutlich weniger Instanzen pro Klasse notwendig sein, um diese zu erlernen, wodurch die Trainingszeiten von einzelnen Klassen erheblich reduziert wird. Deshalb kann dieser Algorithmus von theoretischer Perspektive aus in Echtzeit trainiert werden. In Tabelle 3 sind die genannten Behauptungen im Vergleich zu einem traditionellen DNN nach [2] dargestellt.

Tabelle 3: Übersicht der behaupteten Vorteile des L DNN Algorithmus gegenüber traditionellen DNNs

|  |  |  |
| --- | --- | --- |
|  | Traditionelles DNN | Lifelong DNN Algorithmus |
| Kontinuierliches Lernen | Nein | Ja |
| Lernen auf Endgeräten | Nein | Ja |
| Datenspeicherung notwendig nach Auslieferung | Ja | Nein |
| Datenanforderung | 1000 – 10000 Instanzen pro Klasse  Tausende von Präsentationen pro Instanz | 10 – 100 Instanzen pro Klasse  Eine Präsentation pro Instanz |
| Trainingszeit | Tage – Wochen – Monate | Sekunden |

Eine weitere große Behauptung ist, dass auch bei mehreren verteilten Geräten kein Austausch der Daten notwendig ist. Es werden lediglich Parameter ausgetauscht, welche zwar in gewisser Weise eine abstrahierte Darstellungsform der Daten sind, jedoch keinen direkten Rückschluss auf die Daten zulassen. Damit kann erlerntes Wissen auf Basis von sicherheitskritischen oder persönlichen Daten ausgetauscht werden, ohne dass diese Daten versendet und/oder kostspielig gespeichert und gesichert werden müssen.

## Nachteile

Da die vorhandene Literatur zu diesem Algorithmus von der verfassenden Firma (Neurala) geschrieben wurde, werden lediglich positive Aspekte ausdrücklich erwähnt und detailliert beschrieben. Veröffentlichungen, welche diesen Ansatz kritisch untersuchen, sind bisher nicht vorhanden. Deshalb kann hier noch nicht von konkreten Nachteilen gesprochen werden, da auf Basis der verfügbaren Literatur nur Vorteile gegenüber klassischen Ansätzen gegeben sind. Dennoch werden in diesem Kapitel Punkte genannt, die nicht zwingend ein Nachteil darstellen, jedoch für eine korrekte und faire Betrachtung des L DNN Algorithmus genannt werden müssen.

Dazu muss zunächst genannt werden, dass trotz dem schnell lernenden Modul B dennoch ein klassisches, zeit- und rechenaufwändiges DNN-Training stattfinden muss. Modul A, welches die Feature für Modul B extrahiert, muss vortrainiert werden. Um eine gute Generalisierung zu erzielen, sollten möglichst viele unterschiedliche Bilder gesehen werden. Dafür wird in der Regel der ImageNet-Datensatz genutzt, welcher 1,3 Millionen Trainingsbilder umfasst. Abhängig von der gewünschten Netzwerkarchitektur kann das Training dieser Architektur auch hier einige Stunden bis Tage in Anspruch nehmen.

Zudem muss erwähnt werden, dass durch das vortrainierte Modul A keine weitere Aufgabe durch den L DNN Algorithmus erlernt werden kann. Das DNN in Modul A ist beispielsweise für die Objektklassifizierung vortrainiert, und erreicht dort sehr gute Performanz. Jedoch wird im weiteren Verlauf lediglich Modul B kontinuierlich angepasst, wodurch die Aufgabe fixiert ist. Dies muss jedoch kein Nachteil sein, da in der Regel der Anwendungsfall bereits vorher bekannt ist.

## Zusammenfassung und Vergleich zu klassischen Ansätzen

Auf Basis der in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** dargestellten Grundlagen zu den einzelnen Gebieten, welche im L DNN Algorithmus aufgegriffen werden (Deep Learning, Continual Learning und Distributed Learning), kann gesagt werden, dass im L DNN Algorithmus bereits bekannte Methoden und Ansätze als Grundlage dienen, und diese dort zu einem neuen Algorithmus kombiniert werden.

Die grundlegende Architektur basiert auf bereits bekannten Dual-Memory Methoden, mit einem langsam (oder gar nicht) lernenden Modul A und einem schnell lernenden Modul B. Modul A ist dabei ein typisches DNN, welche genutzt wird um sinnvolle Features für Modul B auf Basis der Eingangsdaten zu extrahieren. Dieses DNN wird mithilfe standardmäßiger Deep Learning Algorithmen (z.B. Backpropagation) trainiert. Modul B ist ein schnell lernendes Klassifikator-Netzwerk, welches die Fähigkeit besitzt sich anzupassen und neue Klassen mit aufnehmen zu können. Neue Klassen werden über ein sogenanntes „*Nothing I know*“-Konzept gefunden, und benötigen das User-Feedback, um diesen Klassen sinnvolle Labels zuweisen zu können.

Wenn mehrere Geräte denselben L DNN Algorithmus nutzen, können diese Geräte sich untereinander austauschen und ihr Wissen weitergeben. Die grundlegende Idee dabei folgt dem Ansatz des *Federated Learning*. Mit diesem Ansatz können sich einzelne Netzwerke auf Basis lokal verfügbarer Trainingsdaten separat trainieren. Die erlernten Parameter werden wiederum mit einem zentralen Server oder unter den einzelnen Geräten ausgetauscht. Dadurch kann das Wissen konsolidiert und über alle Geräte verteilt werden. Mithilfe dieses Ansatzes können Geräte unabhängig von den Daten ihr erlerntes Wissen austauschen, und sicherheitskritische oder persönliche Daten müssen nicht langfristig auf einem Server hochgeladen und gespeichert werden.

Durch die Kombination dieser bereits bekannten Ansätze besitzt der L DNN Algorithmus das theoretische Potenzial eine Vielzahl von Anwendungen bedienen zu können. Dieses Potenzial soll nun im weiteren Verlauf der Arbeit mithilfe des beispielhaften Anwendungsfall der Objekterkennung untersucht und bewertet werden.

# Konzeption

In diesem Dokument wird die konkrete Konzeption des Lifelong DNN (L DNN) Algorithmus beschrieben. Dafür werden unterschiedliche Architekturen untersucht, verglichen und schließlich eine konkrete Architektur ausgewählt, welche im weiteren Verlauf der Arbeit implementiert wird.

Im Folgenden werden nun unterschiedliche Architekturen für die einzelnen Module A und B aufgeführt, verglichen und schließlich für die in dieser Arbeit gestellten Anforderungen bewertet.

## Modul A

Modul A ist das langsame (oder nicht) lernende Modul innerhalb des L DNN Algorithmus. Es ist ein klassisches DNN, welches zur Extraktion von relevanten Features auf Basis von Eingangsdaten genutzt wird. Im Rahmen dieser Arbeit werden vortrainierte, feste DNN-Architekturen genutzt, da das Trainieren solcher DNN-Architekturen sehr zeit- und rechenaufwändig ist.

Es gibt eine Vielzahl an DNN-Architekturen, die heutzutage zur Feature-Extraktion eingesetzt werden. Jede Architektur erfüllt dabei unterschiedliche Anforderungen, beziehungsweiße nutzt unterschiedliche Ansätze, die für den einen oder anderen Anwendungsfall besser geeignet sind. Für Modul A innerhalb des L DNN Algorithmus ist wichtig, dass die extrahierten Features eine bestmögliche Klassifikation erlauben. Zudem soll das System auch in Echtzeitsystemen auf mobilen Endgeräten (z.B. Smartphone) funktionieren [1], [2]. Dafür muss Modul A Eingangsdaten schnell verarbeiten können und gleichzeitig darf der Speicher- und Rechenbedarf des Netzwerkes nicht zu groß sein, da sowohl Speicher als auch Rechenleistung auf mobilen Endgeräten limitiert ist.

Im Folgenden werden bekannte Klassifikator-Netzwerke auf Basis von DNN Architekturen vorgestellt und auf deren Einsetzbarkeit in dieser Arbeit verglichen. Als Grundlage für den späteren Vergleich und für die genannten Metriken wird der Bilddatensatz ImageNet [32] genutzt. Mit ca. 1,2 Millionen Bildern aus 1000 verschiedenen Klassen stellt ImageNet ein sehr komplexes Problem dar. Vortrainierte Netzwerke, welche zur Extraktion von Features genutzt werden, sind heutzutage auf diesem Datensatz trainiert, da er aufgrund seiner großen Anzahl an Trainingsbildern und Klassen eine gute Generalisierung der extrahierten Features gewährleistet.

### AlexNet

AlexNet war eines der ersten DNNs welches die Klassifikationsgenauigkeit auf ImageNet signifikant erhöhte. Im Rahmen der ILSVRC 2012 (*ImageNet Large Scale Visual Recognition Competition*) erreichte AlexNet einen Top-5 Klassifikationsfehler von 15,3%. Der zweitplatzierte dieses Wettbewerbs erreichte lediglich einen Top-5 Klassifikationsfehler von 26%. Es konnte eine erhebliche Steigerung der Klassifikationsgenauigkeit erzielt werden. Dabei ist AlexNet im Vergleich zu aktuellen Architekturen sehr simpel, mit lediglich fünf Convolutional, verschiedenen Max-Pooling sowie drei Fully Connected Schichten [33], [34]. Neuerungen im Vergleich zu damaligen DNNs war der Einsatz von ReLU-Aktivierungsfunktionen sowie die Regularisierung des Netzwerks mithilfe von Dropout [35]. Beide Methoden sind seitdem in nahezu allen DNN-Architekturen im Einsatz. Das Netzwerk besteht aus 60 Millionen Parametern und 650.000 Neuronen. In Abbildung 16 ist die Modellarchitektur des AlexNet graphisch dargestellt, bei welcher die fünf Convolutional und die drei Fully Connected (Dense) Schichten zu sehen sind.

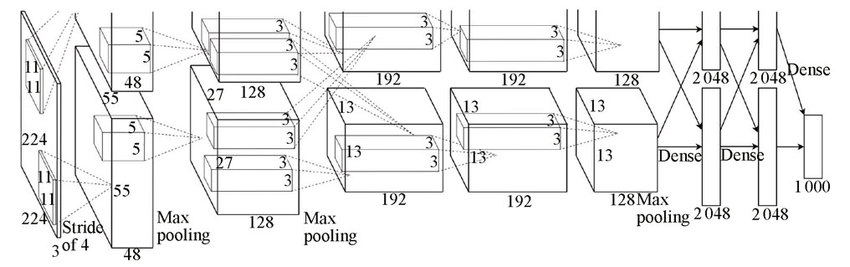


Abbildung 16: Modelarchitektur des AlexNet [34]

Die *Default*-Größe eines Parameters (Floating Point oder Integer) in TensorFlow ist mit 32-bit angegeben [36]. Unter der Annahme dieser Parametergröße benötigt AlexNet mit 60 Millionen Parametern 240 MB Speicher zur Sicherung des Modells. Um die Berechnungskomplexität vergleichen zu können wird die notwendige Anzahl an Operationen für ein einzelnes Eingangselement (z.B. einzelnes Bild) genutzt. Dabei wird lediglich der Vorwärtspfad in Betracht gezogen, wie es bei der späteren Anwendung (*Inference*) des Netzwerkes auch wäre. Diese Anzahl ist bekannt als Nummer von FLOPs (**F**loating **P**oint **OP**erations). AlexNet benötigt 727x106 FLOPs um alle notwendigen Berechnungen im Vorwärtspfad durchzuführen.

### VGG

Die sogenannten VGG-Architekturen entstammen der *Visual Geometry Group* (VGG) der Universität Oxford. Dabei gibt es einige bekannte Architekturen. Die am häufigsten genutzten sind das VGG-16 sowie das VGG-19 Netzwerk. Die Zahlen stehen dabei für die Anzahl an Gewichts-/Parameterschichten innerhalb des DNN. Von der grundsätzlichen Architektur ähnelt es dem bereits beschriebenen AlexNet. Der große Unterschied ist der Einsatz kleinerer Kernel-Filter in den *Convolutional* Operationen (3x3 Kernel anstatt z.B. 11x11 oder 5x5 Kernel in AlexNet). Zudem werden mehrere dieser *Convolutional* Schichten hintereinander gesetzt, wodurch die finale Funktion des DNN diskriminativer werden soll. Ein großer Vorteil ist die geringere Anzahl an Parametern. Unter der Annahme, dass der Eingang und Ausgang eines *Convolutional Stacks* mit drei 3x3 *Convolutional* Schichten Kanäle besitzt, werden Parameter benötigt. Wird lediglich eine einzelne *Convolutional* Schicht mit 7x7 Kernel-Filtern genutzt, werden Parameter benötigt [35]. Durch diese Parameterreduzierung können tiefere Netzwerke mit mehr Schichten aufgebaut werden ohne einen signifikant erhöhten Speicherbedarf zu haben. Durch den Anstieg der Tiefe des Netzwerks ist das Netzwerk fähig komplexere Features zu erlernen [37]. Unterschiedliche Architekturen der VGG-Netzwerke für den ImageNet Bilddatensatz mit 1000 Klassen und RGB Bildern der Größe 224x224 sind in Tabelle 4 dargestellt.

Tabelle 4:VGG-Netzwerk Architekturen [37]

|  |  |  |  |
| --- | --- | --- | --- |
| A  11 Gewichts-Schichten | B  13 Gewichts-Schichten | C  16 Gewichts-Schichten | D  19 Gewichts-Schichten |
| Eingangssignal (z.B. 224x224 RGB Bild) | | | |
| Conv3-64 | Conv3-64  Conv3-64 | Conv3-64  Conv3-64 | Conv3-64  Conv3-64 |
| Max-Pooling | | | |
| Conv3-128 | Conv3-128  Conv3-128 | Conv3-128  Conv3-128 | Conv3-128  Conv3-128 |
| Max-Pooling | | | |
| Conv3-256  Conv3-256 | Conv3-256  Conv3-256 | Conv3-256  Conv3-256  Conv3-256 | Conv3-256  Conv3-256  Conv3-256  Conv3-256 |
| Max-Pooling | | | |
| Conv3-512  Conv3-512 | Conv3-512  Conv3-512 | Conv3-512  Conv3-512  Conv3-512 | Conv3-512  Conv3-512  Conv3-512  Conv3-512 |
| Max-Pooling | | | |
| Conv3-512  Conv3-512 | Conv3-512  Conv3-512 | Conv3-512  Conv3-512  Conv3-512 | Conv3-512  Conv3-512  Conv3-512  Conv3-512 |
| Max-Pooling | | | |
| FC-4096 | | | |
| FC-4096 | | | |
| FC-1000 | | | |
| Softmax | | | |

Wie bereits geschrieben werden die Netzwerke anhand der Anzahl der Gewichtsschichten (*Convolutional* oder *Fully Connected* (FC) Schicht) benannt. So ist Netzwerk *C* als VVG-16 bekannt und Netzwerk D als VGG-19. Die häufig eingesetzten Feature-Extrahierer VGG-16 und VGG-19 werden im Folgenden bezüglich ihres Speicherbedarfes und der Klassifikationsgenauigkeit auf ImageNet untersucht. Dabei sind in Tabelle 5 die Werte der unterschiedlichen Kriterien für die einzelnen Netzwerke gelistet [37].

Tabelle 5: Vergleich von VGG-16 und VGG-19

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Netzwerk-Architektur | Anzahl Parameter | Speicher-bedarf  Parameter | Anzahl  FLOPs | Top-1 Klassifikationsfehler | Top-5 Klassifikationsfehler |
| VGG-16 | 138x106 | 552 MB | 16x109 | 25.6 % | 8.1 % |
| VGG-19 | 144x106 | 576 MB | 20x109 | 25.5 % | 8.0 % |

Die Anzahl der Parameter, und damit auch der Speicherbedarf, steigt mit der Anzahl an Schichten. Hinsichtlich des Klassifikationsfehlers auf ImageNet ist zu beobachten, dass durch die 3 zusätzlichen Schichten im VGG-19 Netzwerk ein nahezu vernachlässigbarer Genauigkeitsgewinn erreicht werden kann. Es werden 6 Millionen zusätzliche Parameter (24MB zusätzlicher Speicher) sowie 4x109 zusätzliche FLOPs benötigt, um den Top-1 und Top-3 Klassifikationsfehler um 0.1% zu verringern.

### ResNet

Aufgrund der bisher beschriebenen Modelle kann die Aussage getroffen werden, dass eine größere Tiefe des Netzwerks eine bessere Genauigkeit ermöglicht. Bei diesen Überlegungen muss jedoch berücksichtigt werden, dass bei der Backpropagation der Error-Vektoren durch das Netzwerk viele Schichten durchlaufen werden müssen. Dies führt dazu, dass der Error, der bei frühen Schichten ankommt, sehr klein oder gleich null ist und damit nur eine geringe oder gar keine Anpassung der Parameter stattfindet. Dieses Problem ist in der Literatur unter dem Namen *Vanishing Gradient* (Verschwindender Gradient) bekannt. Zusätzlich wurde bei sehr tiefen neuronalen Netzwerken das Degradations-Problem beobachtet. Mit einer zunehmenden Netzwerk-Tiefe findet eine Sättigung in Bezug auf die Genauigkeit des Netzwerkes statt. Ab einem gewissen Punkt degradiert diese Genauigkeit schließlich. Dieses Verhalten lässt darauf schließen, dass nicht alle Netzwerke beliebiger Architektur gleich zu trainieren sind.

Um diese genannten Probleme zu lösen, wurden *Deep Residual Networks*, häufig nur als ResNet (Residual Network) bezeichnet, eingeführt [38]. Diese ResNets nutzen dieselben grundlegende Schichten wie VGG-Netze, mit kleinen Kernel-Filter (3x3) und hauptsächlich *Convolutional* Schichten. ResNets bestehen zusätzlich aus einer Vielzahl von *Residual* Blöcken. Ein solcher *Residual* Block ist beispielhaft in Abbildung 17 dargestellt.



Abbildung 17: Beispielhafter Residual Block [38]

Diese *residual* Blöcke verwirklichen das gewünschte Verhalten des Eingangssignals mithilfe der non-linearen Verarbeitung und der Hinzunahme des ursprünglichen Eingangssignals **,** wodurch gilt: . Die Hinzunahme des Eingangssignals wird mithilfe von sogenannten *Shortcut Connections* realisiert. In den meisten ResNets entspricht die *Shortcut Connection* dabei dem Identity Mapping, in der Theorie kann diese Verbindung jedoch auch einen zusätzlichen Operator beinhalten. Mithilfe dieser Netzwerke können zum einen tiefe Netzwerke (mit mehr als 100 Schichten) effizient und schnell trainiert werden, zum anderen kann die Genauigkeit dieser Netzwerke weiter erhöht werden, da das Potenzial der zusätzlichen tiefen Schichten genutzt wird und keine Degradation stattfindet. Damit kann sowohl das Problem des *Vanishing Gradient*, als auch das *Degradation Problem* gelöst werden [38].

Ein Ausschnitt einer beispielhaften ResNet-Architektur ist in Abbildung 18 gegeben. Es sind exemplarisch nur die ersten Schichten dargestellt. Links ist als Referenz die Architektur des VGG-19 Netzwerks zu sehen. In der Mitte ist ein „normales“ DNN mit 34 Schichten gezeigt und rechts das dazu passende ResNet, ebenfalls mit 34 Schichten aber bestehend aus *residual* Blöcken.

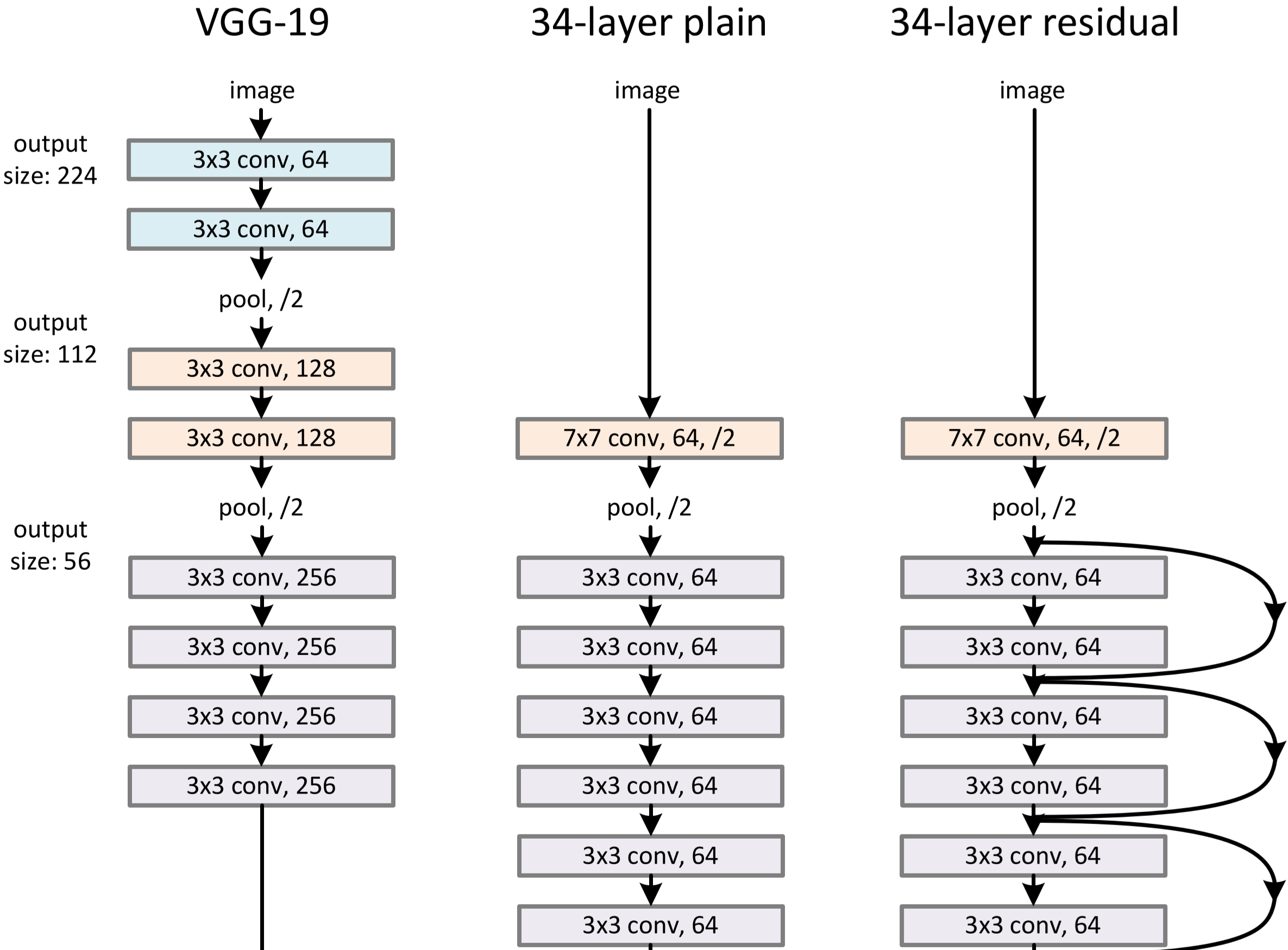


Abbildung 18: Beispielhafte Architektur VGG-19 (links), Standard-Architektur (mitte), ResNet (rechts) [38]

Für das Beispiel von 34 Schichten kann auf Basis des ImageNet Datensatzes der Top-1 Klassifikationsfehler von 28.54% im Falle des *plain* Netzwerks auf 25.03% mithilfe des ResNets reduziert werden. Die gesamte Modellarchitektur (Anzahl Parameter, Schichten, Multiplikationen…) ist dabei identisch, lediglich die *Shortcut Connections* sind zusätzlich eingefügt. Ein ResNet kann mit einer beliebigen Anzahl an Schichten aufgebaut werden. In dieser Arbeit werden als Referenzen eine Architektur mit 50 und 101 Schichten angegeben. Die Anzahl an Parameter, der benötigte Speicherbedarf bei Umsetzung in TensorFlow [36], sowie der Top-1 und Top-5 Klassifikationsfehler auf dem ImageNet Datensatz nach [38] sind in Tabelle 6 angegeben.

Tabelle 6: Vergleich von ResNet-50 und ResNet-100

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Netzwerk-Architektur | Anzahl Parameter | Speicher-bedarf Parameter | Anzahl FLOPs | Top-1  Klassifikationsfehler | Top-5  Klassifikationsfehler |
| ResNet-50 | 25.6x106 | 102 MB | 4x109 | 20.7 % | 5.3 % |
| ResNet-101 | 44.5x106 | 178 MB | 8x109 | 19.9 % | 4.6 % |

Im Vergleich zu den bereits eingeführten Architekturen (VGG oder ALexNet) kann hier mit weniger Speicherbedarf (geringerer Anzahl an Parametern) sowie deutlich weniger FLOPs dank der *Residual Blocks* eine bessere Genauigkeit auf dem ImageNet-Datensatz erreicht werden.

### GoogLeNet/Inception

Mithilfe der VGG-Architekturen konnte ein bemerkenswerter Sprung bei der Genauigkeit von DNNs auf dem ImageNet-Datensatz erzielt werden. Um diese VGG Netzwerke trainieren zu können bedarf es jedoch aufgrund der hohen Anforderungen für die Berechnung sehr teure Hardware (GPUs). An diesem Punkt setzt der Aufbau des GoogLeNet an, häufig auch als Inception Netzwerk bekannt [39], [40]. GoogLeNet nutzt die Idee, dass die meisten Aktivierungen in einem DNN entweder unnötig (Aktivierung gleich 0) oder aufgrund von Korrelationen redundant sind. Daher ist die effizienteste Architektur eines DNN ein Aufbau mit sparsen Verbindungen zwischen den Aktivierungen. Das bedeutet, dass nicht alle Ausgangskanäle mit allen Eingangskanälen in einer *Convolutional* Schicht verbunden sind, wie es typischerweise der Fall wäre [35]. GoogLeNet setzt dafür sogenannte Inception-Module ein, welche ein sparses CNN mit normalen Konstruktionen approximieren. Der Aufbau eines Inception-Moduls ist in Abbildung 19 dargestellt.

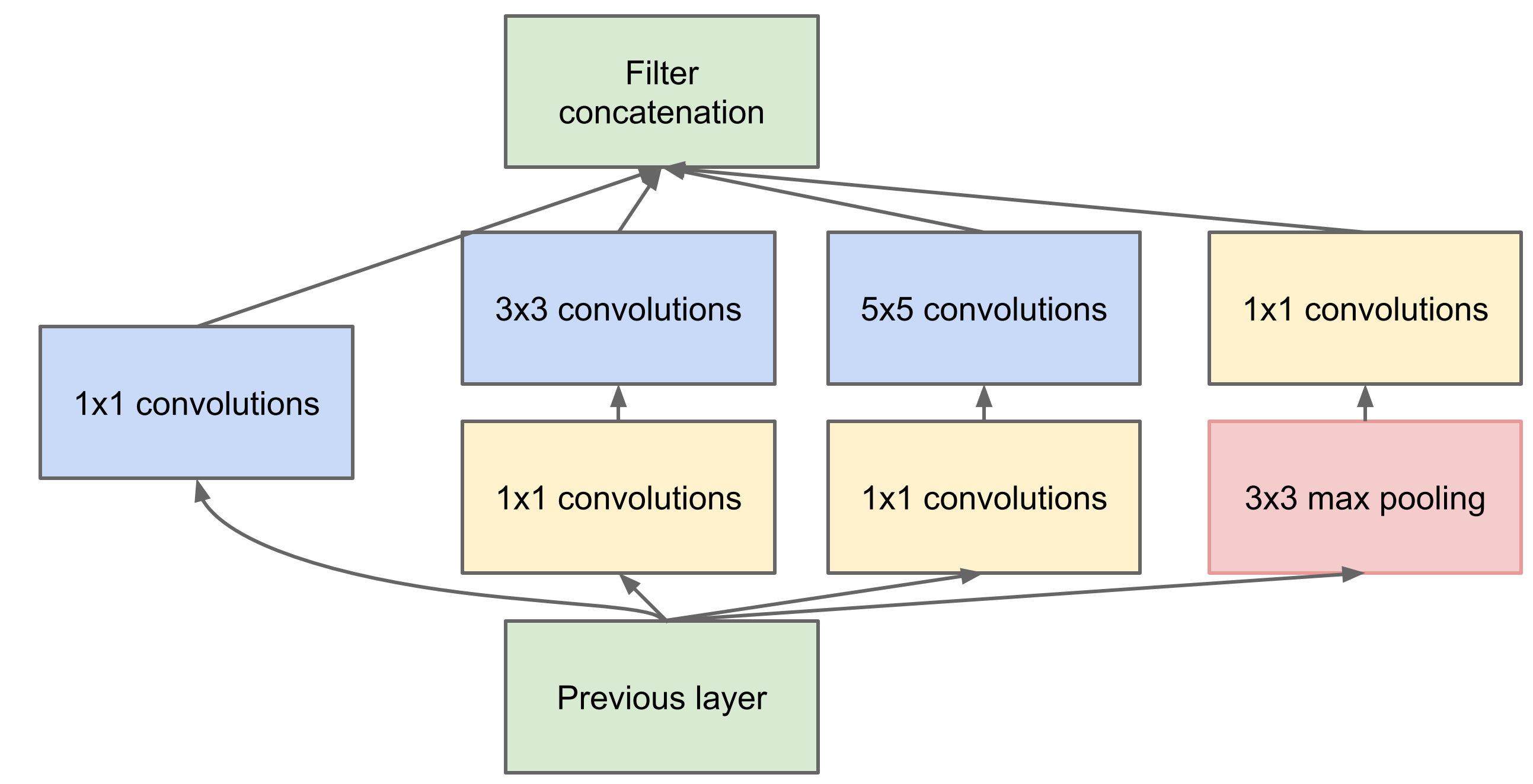


Abbildung 19: Inception-Modul [39]

Mithilfe dieser Architektur kann die Anzahl an benötigten Operationen (Multiplikation, Additionen) deutlich reduziert werden. Die 1x1 *Convolutions* dienen dabei der Dimensionsreduzierung der Kanäle, bevor größere Convolutional-Operationen (3x3 oder 5x5) durchgeführt werden. Als einfaches Beispiel kann dafür eine Berechnung von 192 Eingangskanälen an der 5x5 Convolution gesehen werden. Mit 32 Filtern würden Multiplikationen durchgeführt. Wird zuvor eine 1x1 Convolution mit 16 Filtern genutzt, sind nur Multiplikationen notwendig um dieselbe Ausgangsdimension zu erhalten. Mithilfe der Inception-Module kann ein sehr tiefes und weites Netz (große Eingangsdimensionen) aufgebaut werden. Zusätzlich zu diesen Änderungen verzichtet GoogLeNet auf Fully-Connected Schichten am Ende des Netzwerkes, und tauscht diese durch Pooling-Operationen aus. Dies reduziert die Anzahl an benötigten Parametern drastisch. Im AlexNet sind z.B. ca. 90% der Parameter in den Fully Connected Schichten enthalten [35].

Die dritte Version des Inception-Netzwerks (Inception-v3 [40]) besitzt 42 Schichten und erreicht einen Top-5 Klassifikationsfehler von 5.6% und einen Top-1 Klassifikationsfehler von 21.2%. Dabei werden 4.8x109 FLOPs ausgeführt und 24x106 Parameter genutzt. Unter der Annahme von 32-bit Variablen [36] ergibt das einen Speicherbedarf von 96 MB.

### MobileNet

Der Trend im Bereich DNN ist es, immer tiefere und komplexere Netzwerke zu gestalten, welche verbesserte Genauigkeiten für spezifische Aufgaben (z.B. ILSVRC) liefern. Als Folge von diesen Entwicklungen steigt häufig der Berechnungsaufwand und/oder der Speicherbedarf zur Umsetzung dieser Netzwerke. In vielen realen Anwendungen sind jedoch genau diese Themen kritisch, z.B. für Augmented Reality, autonome Fahrzeuge, Roboter und vieles mehr. In diesen Anwendungsgebieten sind echtzeitfähige Netzwerke notwendig, die auf kleinen Endgeräten (z.B. Smartphone oder Mikrocontroller) lauffähig sind, und keinen GPU-Server zur Verfügung haben. Aus diesen Anforderungen heraus wurde MobileNet [41] entworfen. Das Ziel der Architektur ist ein kleines Netzwerk mit geringer Latenz, dass für mobile Anwendungen genutzt werden kann. MobileNet nutzt dabei auch Inception-Module [39] um die Anzahl an Operationen zu reduzieren. Zusätzlich wird die *Depthwise Separable Convolution* eingesetzt. Dies ist eine Form der faktorisierten *Convolution*, bei dem die normale *Convolution* in eine *depthwise Convolution* und eine 1x1 *Convolution* (*pointwise* Convolution) zerlegt wird. Dadurch werden aus einer Schicht zwei Schichten, bei der die erste für die Filterung und die zweite für die Kombination der berechneten Filterausgänge verantwortlich ist [41]. Als Vergleich ist in Tabelle 7 der Unterschied für die Anzahl an FLOPs, der Anzahl der Parameter und der Genauigkeit auf dem ImageNet-Datensatz für ein MobileNet mit klassischen *Convolution*-Operatoren (Conv MobileNet) und einem MobileNet, welches *depthwise Convolutions* nutzt, gegeben.

Tabelle 7: Depthwise Separable vs. Full Convolution MobileNet [41]

|  |  |  |  |
| --- | --- | --- | --- |
| Modell | Top-1 Klassifikationsfehler | Anzahl FLOPs | Anzahl Parameter |
| Conv MobileNet | 28.3% | 4.87x109 | 29.3x106 |
| MobileNet | 29.4% | 0.57x109 | 4.2x106 |

Diese Ergebnisse zeigen, dass der Einsatz der d*epthwise Convolution* den Speicher- und Rechenaufwand drastisch reduziert, und der daraus resultierende Genauigkeitsverlust bei lediglich ca. 1% liegt, was angesichts der Reduzierung der Aufwände allgemein akzeptiert werden kann.

In [42] wird eine verbesserte Version 2 des MobileNets, MobileNet-V2, vorgestellt. Dabei werden zusätzlich zu den bereits beschriebenen Modulen neue Module eingesetzt, die zum einen den Speicherbedarf reduzieren und zum anderen die Performanz steigern sollen. Dies geschieht durch den Einsatz von *Inverted Residuals* mit *Linear Bottelenecks*. Die *Linear Bottlenecks* sorgen dafür, dass keine großen Tensoren zwischen den Schichten über *Shortcut* Verbindungen übergeben werden, sondern sorgen mithilfe einer linearen Transformation für ein *Bottleneck*. Durch die lineare Transformation soll sichergestellt werden, dass relevante Informationen nicht durch eine nicht-lineare Dimensionsreduktion verloren gehen. Die *Inverted Residual* Blöcke nutzen klassische *Shortcut* Verbindungen und deren Vorteile des verbesserten Gradienten-Flusses [38]. Das invertierende ist die Stelle, an denen diese Verbindungen eingesetzt werden. Typischerweise sind bei *Shortcut*-Verbindungen zwei hochdimensionale Blöcke verbunden, zwischen denen ein *Bottleneck* liegt. Bei den *Inverted Residual* Blöcken sind zwei *Bottlenecks* verbunden, zwischen denen ein höherdimensionaler Block liegt. Dadurch soll der Speicherbedarf weiter reduziert werden, da niederdimensionale Blöcke (die *Bottlenecks*) über die *Shortcut*-Verbindung weitergeleitet werden anstatt hochdimensionaler Tensoren. In Abbildung 20 ist die Architektur des MobileNet-V2 vereinfacht graphisch dargestellt. An dieser Abbildung lässt sich gut der Aufbau der beschriebenen *Inverted Residual* mit *Linear Bottlenecks* erkennen.

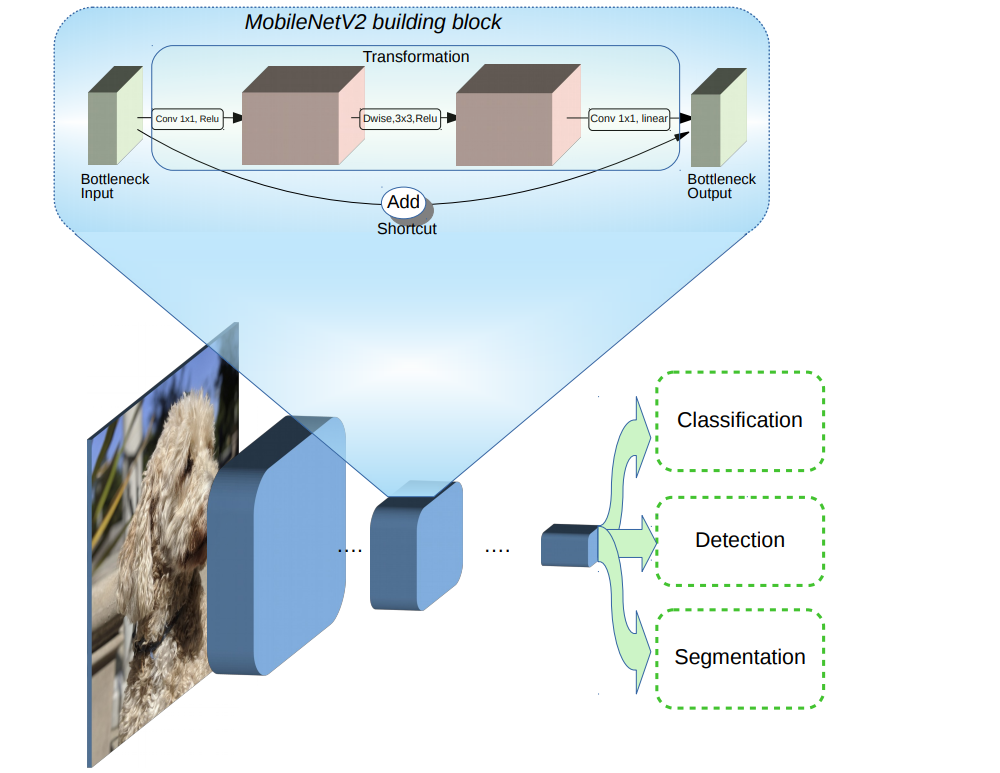


Abbildung 20: Schematische Übersicht über MobileNet-V2 Architekture [43]

MobileNet-V2 erreicht einen Top-1 Klassifikationsfehler von 28% und einen Top-5 Klassifikationsfehler von 9%. Das Modell besteht aus 3.5x106 Parametern (entspricht 14 MB Speicher) und führt 0.3x109 FLOPs pro Eingangsbild aus [42], [43].

## Modul B

Wie in den Grundlagen bereits beschrieben wird Modul B des L DNN Algorithmus mithilfe eines inkrementellen Klassifikators realisiert. Zu den grundlegenden Anforderungen eines inkrementellen Klassifikators, die ebenfalls in den Grundlagen beschrieben wurden, kommen in dieser Arbeit weitere spezifische Anforderungen. Es ist in dieser Arbeit relevant, dass der inkrementelle Klassifikator ohne Speicherung vorheriger Eingangsdaten arbeitet. Dafür gibt es zwei konkrete Gründe.

Zum einen sind Anwendungen interessant, bei denen die Algorithmen auf mobilen Endgeräten laufen. Diese haben nur begrenzten Speicher zur Verfügung und können nicht eine Vielzahl von Daten sichern. Zudem fallen bei Echtzeit-Anwendungen enorm viele Daten an, die nicht ohne einen großen Daten-Server gespeichert werden können. Ein Transfer dieser Daten auf einen Server würde jedoch einen erheblichen Kommunikationsaufwand darstellen.

Als zweiten Punkt kann der Einsatz in sicherheitsrelevanten Anwendungen genannt werden. Es kann dabei zwischen sicherheitskritischen Daten und persönlichen Daten unterschieden werden. Beide müssen bei einer Sicherung mit hohem Aufwand geschützt werden. Dies kann auf mobilen Endgeräten nicht immer sichergestellt werden. Bei einer Kommunikation zu einem Server muss wiederum eine sichere Verbindung gewährleistet werden.

Da diese Punkte hohe Aufwände verursachen, soll der inkrementelle Klassifikator nicht mit abgespeicherten Beispieldaten arbeiten, wodurch die genannten Probleme umgangen werden können.

Die beschriebenen Klassifikatoren, Incremental Classifier and Representation Learning (iCaRL) und Adaptive Resonance Theory (ART), erfüllen beide die in [24] gestellten Anforderungen an einen inkrementellen Klassifikator:

* Er soll auf Basis eines Daten-Stream, in dem Sample der unterschiedlichen Klassen zu unterschiedlichen Zeitpunkten (zufällig) auftreten, trainierbar sein
* Zu jedem Zeitpunkt muss ein funktionierender Multi-Klassen Klassifikator für die bereits gesehenen und damit bekannten Klassen verfügbar sein
* Die Berechnungsanforderungen und der Speicherbedarf sollen beschränkt sein oder nur langsam ansteigen mit Bezug auf die Anzahl an bekannten Klassen

Jedoch benötigt iCaRL für die Berechnungen der Repräsentationen eine ausgewählte Menge an Exemplaren der jeweiligen Klassen. Diese Anzahl an gespeicherten Daten pro Klasse kann variieren, jedoch wird eine Anzahl von 10 bis 20 Exemplaren pro Klasse empfohlen [44]. Dies widerspricht den oben eingeführten Kriterien, keine spezifischen Daten sichern zu müssen. Zudem müssen für einen Austausch von Wissen zwischen einzelnen, verteilten Netzen diese gespeicherten Exemplare ebenfalls ausgetauscht werden. Aus diesem Grund wird in dieser Arbeit iCaRL nicht für die Umsetzung von Modul B genutzt.

ART-Netzwerke sichern ebenfalls Repräsentationen von Klassen, jedoch keine einzelnen Eingangsdaten von Klassen. Es wird eine Repräsentation pro Klasse angelegt, und inkrementell generalisiert, wenn neue Daten für diese Klasse eintreffen. Durch die Generalisierung der Daten können einzelne Eingangsdaten nicht rückverfolgt werden, weshalb die gestellten Anforderungen für Modul B erfüllt werden können.

Durch den Einsatz des in [1] vorgestellten „*Nothing I Know*“-Konzepts können neue, bisher unbekannte Klassen erkannt werden und ein neuer Knoten für diese Klasse erstellt werden. Bei diesem Punkt muss erwähnt werden, dass vor Beginn der Anwendung eine Anzahl an maximal möglichen Klassen festgelegt werden muss, da die Anzahl an verfügbaren Knoten (Neuronen) in einem ART-Netzwerk initial festgelegt wird. Somit können nicht beliebig viele Klassen inkrementell erlernt werden, aber es kann durch eine vorherige Abschätzung eine ausreichende Anzahl vorgegeben werden.

Es gibt eine Vielzahl an unterschiedlichen ART-Netzwerken, welche jeweils für verschiedene Anwendungen genutzt werden. In dieser Arbeit wird ein Fuzzy ARTMAP (FAM)-Netzwerk genutzt. Der Hauptvorteil besteht darin, dass durch den Einsatz der Fuzzy-Theorie anstatt binärer Vektoren (wie in einem klassischen ART1-Netzwerk) kontinuierliche Werte im Bereich zwischen 0 und 1 genutzt werden können. Zudem werden die Fuzzy-Operatoren eingesetzt. In einem FAM-Netzwerk ersetzt dabei der Fuzzy-AND Operator den binäre AND Operator. Der Fuzzy-AND Operator ist dabei wie folgend definiert: [26].

Zusätzlich arbeitet ein typisches FAM-Netzwerk mit komplementärer Codierung (*complement coding*), wodurch ein ursprüngliches Eingangssignal umgewandelt wird zu , mit dem komplementären Eingangssignal , das an das originale Eingagssignal angehängt wird [26].

Nach [1] sind diese eben genannten Besonderheiten der Fuzzy-Operatoren und des *complement Coding* auch Probleme bei der Nutzung eines solchen Netzwerkes innerhalb des L DNN Algorithmus. Da DNNs als Feature Extrahierer zu sparsen Feature Repräsentationen tendieren, führt der Einsatz von komplementärer Codierung zu sehr hohen Aktivierungen im komplementären Teil. Kleine Unterschiede zwischen einzelnen Mustern lassen sich dann schwierig unterscheiden. Deswegen wird in [1] vorgeschlagen, den *complement Coding* Teil des FAM-Netzwerks nicht zu nutzen, was in dieser Arbeit übernommen wird. Als zusätzliche Maßnahme wird der Austausch der Fuzzy AND Logik durch das Skalarprodukt von zwei Vektoren vorgeschlagen. Dadurch kann erzielt werden, dass das Ergebnis der Vergleichsoperation normalisiert ist.

Aufbauend auf diesen Änderungen wird in dieser Arbeit eine weitere Adaption des FAM-Netzwerkes genutzt, das Simplified FAM (SFAM)-Netzwerk [45]. Das SFAM benötigt zur Initialisierung im Gegensatz zu den anderen ART-Netzwerk lediglich die Toleranzschwelle (*Vigilance Parameter*) . Wenn während des Trainings festgestellt wird, dass dieser Parameter zu niedrig ist und es deshalb zu Fehlklassifizierungen kommt, wird dieser Parameter automatisch nach oben angepasst. Dieser Fall wird *Category Mismatch* genannt und stellt die Besonderheit des SFAM-Netzwerkes dar [26]. Mit dieser Konzeption des Modul B können die gestellten Anforderungen in der Theorie bewältigt werden. Eine graphische Darstellung und eine kurze Zusammenfassung werden in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** gegeben.

## Zusammenfassung

In diesem Kapitel werden eine Zusammenfassung und finale Bewertung der unterschiedlichen Ansätze für die jeweiligen Module gegeben. Es wird auf Basis der eingesetzten Metriken und genannten Kriterien jeweils ein Ansatz pro Modul ausgewählt. Abschließend wird dann der gesamte Lifelong DNN Algorithmus mit den ausgewählten Modulen dargestellt.

### Modul A

Modul A hat wie in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** beschrieben unterschiedliche Kriterien, die ausschlaggebend für die Auswahl sind. Es gibt eine Vielzahl an möglichen Netzwerken, welche die Aufgaben von Modul A übernehmen können. Die konkrete Auswahl ist stark vom gewünschten Anwendungsfall und der gegebenen Hardwareumgebung abhängig. In Tabelle 8 sind alle vorgestellten DNN-Architekturen nochmals direkt miteinander verglichen.

Tabelle 8: Übersicht aller vorgestellten DNNs für Modul A

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Netzwerk-Architektur | Anzahl Parameter | Speicher-bedarf  Parameter | Anzahl  FLOPs | Top-1 Klassifikationsfehler | Top-5 Klassifikationsfehler |
| AlexNet | 60x106 | 240 MB | 0.7x109 | 36.7 % | 15.3 % |
| VGG-16 | 138x106 | 552 MB | 16x109 | 25.6 % | 8.1 % |
| VGG-19 | 144x106 | 576 MB | 20x109 | 25.5 % | 8.0 % |
| ResNet-50 | 25.6x106 | 102 MB | 4x109 | 20.7 % | 5.3 % |
| ResNet-101 | 44.5x106 | 178 MB | 8x109 | 19.9 % | 4.6 % |
| Inception-V3 | 24x106 | 96 MB | 4.8x109 | 21.6 % | 5.6 % |
| MobileNet-V2 | 3.5x106 | 14 MB | 0.3x109 | 28 % | 9 % |

Im Rahmen dieser Arbeit gibt es keine limitierenden Hardware-Begrenzungen. Dennoch soll berücksichtigt werden, dass der implementierte Lifelong DNN Algorithmus auch auf mobilen Endgeräten (z.B. Smartphone oder Mikrocontroller) lauffähig sein soll.

Zunächst wird deshalb der berechnete Speicherbedarf der Netzwerke verglichen. Hier gibt es eine große Schwankung zwischen 576 MB für VGG-19 und 14 MB für MobileNet-V2. Trotzdem kann gesagt werden, dass auch der Speicherbedarf eines VGG-19 Netzwerkes akzeptabel wäre, da Endgeräte heutzutage häufig die Möglichkeit besitzen ein zusätzliches Speichermodul (z.B. SD-Karte) einzusetzen, wodurch zusätzlicher Speicher gewonnen werden kann. Es muss jedoch auch in Relation gesetzt werden, dass z.B. auf Smartphones APPs nur selten größer als 300 MB sind, weshalb VGG-16 und VGG-19 in einigen mobilen Anwendungen nicht die optimale Wahl wäre.

Weiter wird die benötigte Anzahl an Operationen für die Bearbeitung eines einzelnen Eingangsbild verglichen. Auch hier gibt es große Unterschiede, von 20 Giga-FLOPs (GFLOPs) in einem VGG-19 bis zu 0,3 GFLOPs in MobileNet-V2. Dieser Punkt ist für mobile Anwendungen kritischer zu sehen als der Speicherbedarf. Der Grund liegt darin, dass bei vielen mobilen Anwendungen Echtzeitfähigkeit gefordert ist. Um dies zu gewährleisten, müssen die benötigten Operationen für die Bearbeitung von Eingangsdaten von dem vorhandenen Prozessor in einem gewissen Zeitraum (z.B. innerhalb einer Sekunde) abgearbeitet werden. Abhängig vom Anwendungsfall können dabei unterschiedliche Raten erforderlich sein. Im Fall von Bildverarbeitung wird in diesem Kontext von **F**rames **P**er **S**econd (FPS) gesprochen. Für einen konkreten Vergleich wird als Hardware ein in der Praxis häufig genutzter Mikrocontroller, der Raspberry Pi 3 Modul B [46], angenommen. In dem Kontext von FLOPs ist die Taktfrequenz der Hardware relevant, welche für diesen Mikrocontroller mit 1,2 GHz angegeben ist [46]. Unter der Annahme, dass nur die in der Tabelle aufgeführten FLOPs zur Bearbeitung des Eingangsbildes ausgeführt werden müssen, kann eine theoretische FPS-Rate berechnet werden. Mit einem VGG-19 würde ein Raspberry Pi 3 Modul B 0,06 FPS erreichen können. Die Bearbeitung eines Bildes würde somit 16,6 Sekunden brauchen. Mit dem ResNet-50 könnte eine FPS-Rate von 0,3 erreicht werden, und mit MobileNet-V2 nach diesen Überlegungen 4 FPS. Mit einem ResNet-50 würde die Bearbeitung eines Bildes ca. 3,3 Sekunden brauchen. Wenn dies noch als akzeptabel angenommen wird für die Anwendung, wäre auf Basis von diesem Kriterium lediglich AlexNet, ResNet-50 und MobileNet-V2 relevant für die spätere Nutzung.

Als letzten Punkt wird die Genauigkeit der Netzwerke verglichen. Die genannten Netzwerke werden im späteren Verlauf nicht als Klassifikatoren eingesetzt, aber die Klassifikationsgenauigkeit gibt eine gute Übersicht über die Fähigkeit, relevante Features zu extrahieren. Auch hier muss abhängig von der realen Anwendung entschieden werden. Für sicherheitskritische Anwendungen spielt die Genauigkeit eine große Rolle, während für sicherheitsunkritische Anwendungen die Genauigkeit eventuell geringer sein kann und dafür mehr Wert auf eine geringe Laufzeit gelegt wird. Im Rahmen dieser Arbeit wird das generelle Potenzial des Lifelong DNN Algorithmus untersucht und nicht die exakte Performanz von CNN-Architekturen. Deshalb kann auch eine geringere Genauigkeit auf dem ImageNet-Datensatz akzeptiert werden, wenn dafür die anderen, bereits genannten Kriterien die Erwartungen erfüllen.

Unter Berücksichtigung aller genannten Kriterien wird im weiteren Verlauf der Arbeit MobileNet-V2 als Modul A des Lifelong DNN Algorithmus eingesetzt. Dafür spricht die spezielle Architektur für mobile Anwendungen, die eine Echtzeit(nahe)-Bearbeitung von Eingangsdaten auch auf mobilen Endgeräten erlaubt. Dies wird sowohl durch den geringen Speicherbedarf mit lediglich 14 MB, als auch durch die geringe Anzahl von 0,3 GFLOPs, die pro Eingangsdaten ausgeführt werden müssen, gewährleistet. Dadurch kann dieses Netzwerk auch auf leistungsschwächeren Endgeräten laufen. Zudem kann trotz dieser Merkmale ein Top-5 Klassifikationsfehler von 9% auf dem ImageNet-Datensatz erreicht werden, was im Rahmen dieser Arbeit eine ausreichende Genauigkeit darstellt, die auch von vielen komplexeren Netzwerken nicht erreicht wird (z.B. AlexNet) oder nur knapp unterboten wird (z.B. VGG-16 und VGG-19).

Die Architektur des MobileNet-V2 Netzwerks ist in Tabelle 9 aufgeführt.

Tabelle 9: Architektur MobileNet-V2 [42]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Input | Operator | t | c | n | s |
| 224x224x3 | Conv2d | - | 32 | 1 | 2 |
| 112x112x32 | Bottleneck | 1 | 16 | 1 | 1 |
| 112x112x16 | Bottleneck | 6 | 24 | 2 | 2 |
| 56x56x24 | Bottleneck | 6 | 32 | 3 | 2 |
| 28x28x32 | Bottleneck | 6 | 64 | 4 | 2 |
| 14x14x64 | Bottleneck | 6 | 96 | 3 | 1 |
| 14x14x96 | Bottleneck | 6 | 160 | 3 | 2 |
| 7x7x160 | Bottleneck | 6 | 320 | 1 | 1 |
| 7x7x320 | Conv2d 1x1 | - | 1280 | 1 | 1 |
| 7x7x1280 | Avgpool 7x7 | - | - | 1 | - |

Dabei stellt jede Zeile eine Sequenz von einer oder mehreren identischen Schichten dar, die *n*-Mal wiederholt wird. Alle Schichten innerhalb einer Sequenz (Zeile) haben dieselbe Anzahl *c* an Ausgangskanälen. Die erste Schicht einer Sequenz hat dabei die *Stride s* und alle weiteren Schichten dieser Sequenz nutzen *Stride* 1. Alle *spatial Convolutions* nutzen 3x3 Kernel. Der Expansionsfaktor *t* wird auf die Eingangsgröße angewendet, um das Prinzip der linearen Bottlenecks zu nutzen.

Das Netzwerk besteht aus einer initialen *Convolutional* Schicht und darauffolgend 17 Bottleneck Schichten. Zum Schluss folgen eine 1x1 *Convolution* Schicht und eine Pooling-Schicht. Wenn das Netzwerk zur Klassifikation eingesetzt würde, würde noch eine zusätzliche Schicht folgen mit Softmax-Aktivierung. Da hier jedoch die Features nur genutzt werden, wird diese Schicht nicht genutzt. Damit ist der Ausgang von Modul A (und damit der Eingang von Modul B) ein Tensor mit den Dimensionen 1x1x1280, der wiederum direkt in einen Vektor der Größe 1280x1 übertragen werden kann.

### Modul B

Modul B besteht wie in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** beschrieben aus einem Simplified Fuzzy ARTMAP (SFAM) Netzwerk. Dieses Netzwerk kann initial mit bereits bekannten Klassen vortrainiert sein oder initial „leer“ sein (keine Klassen bekannt). Ausgehend davon werden neue Eingangsdaten klassifiziert. Falls die Eingangsdaten zu keiner bekannten Klasse passen, fallen diese Eingangsdaten in die Kategorie „Nothing I know“, und eine neue Repräsentation (neuer Knoten) wird im Netzwerk angelegt. Für diesen Schritt ist das Feedback des Benutzers notwendig, um das korrekte Klassenlabel zu erhalten. Die Architektur des genutzten SFAM-Netzwerks ist in Abbildung 21 dargestellt. Die einzelnen Bestandteile und deren Nutzen werden im Folgenden erläutert.



Abbildung 21: Architektur des SFAM-Netzwerks

Das Eingangssignal der Dimension (Größe) kommt an der Eingangsschicht an. Daraufhin werden die erlernten Gewichte der Kategorieknoten mit diesem Eingangssignal assoziiert. Diese Gewichte werden Top-Down Gewichte genannt, da sie von oben nach unten (Top-Down) mit den Eingangsdaten assoziiert werden. In dieser Arbeit wird wie in [1] vorgeschlagen das Skalarprodukt der Gewichte mit den Eingangsdaten für die Assoziation genutzt. Auf Basis dieser berechneten Assoziationen erfolgen dann die Aktivierungen der Ausgangsneuronen () in der Kategorie Schicht. Abhängig von den erlernten Gewichten können auch mehrere Kategorie-Knoten auf dieselben Ausgangsneuronen zeigen, wenn die einzelnen Kategorie-Knoten dieselbe Klasse repräsentieren. In der Kategorie Schicht wird während des Trainings (der Adaptionsphase) die korrekte Klasse hinzugefügt, um das richtige Label für ein korrektes adaptieren der Neuronen im Netzwerk zu haben.

Die berechneten Aktivierungen (*Matching*-Werte) werden dann mit dem *Vigilance* Parameter verglichen. Wenn dieser Schwellwert überschritten ist, wird die Gewinner-Kategorie/Klasse ausgegeben und somit die Eingangsdaten dieser Klasse zugeordnet. Bei einer Fehlklassifikation (Netzwerkausgabe entspricht nicht bekanntem Label) wird in einem SFAM-Netzwerk der Schwellwert automatisch nach oben angepasst, damit diese Fehlklassifikation in Zukunft nicht mehr auftreten kann. Dadurch werden die Kategorien feiner und es entstehen potenziell mehrere Kategorie-Knoten für dieselbe Klasse.

Wenn das Matching der Gewinner-Kategorie den Schwellwert unterschreitet, findet das *Nothing* *I know*-Konzept Anwendung. Da das höchste Matching nicht ausreichend ist, erkennt das Netzwerk, dass es dieses Eingangsmuster nicht kennt. In diesem Fall wird dann ein neuer Kategorie-Knoten für das gegebene Eingangsmuster angelegt. Der Benutzer muss in diesem Fall die korrekte Kategorie angeben, damit für spätere Eingangsdaten die passende Kategorie-Bezeichnung ausgegeben werden kann.

### Lifelong DNN Algorithmus

Aus den beiden beschriebenen Modulen A und B lässt sich nun der gesamte Lifelong DNN Algorithmus bauen. Er besteht aus einem vortrainierten Feature-Extrahierer, welcher durch das MobileNet-V2 realisiert wird. Dieses Netzwerk wird auf Basis des ImageNet-Datensatzes als Klassifikator vortrainiert. Die letzte Schicht wird dann entfernt, und die extrahierten Features an Modul B, den inkrementellen Klassifikator weitergeleitet. Dieses Modul wird durch ein SFAM-Netzwerk realisiert. Als Ausgabe des Modul B erhält der Benutzer das prädizierte Klassenlabel des Eingangsbildes. Die gesamte Architektur sowie Beispieldimensionen für ein 224x224x3 Eingangsbild sind in Abbildung 22 skizziert.



Abbildung 22: Gesamtarchitektur L DNN Algorithmus

Im weiteren Verlauf der Arbeit werden nun Experimente definiert, um die Performanz des Lifelong DNN Algorithmus sowie dessen Potenzials zu überprüfen. Daraufhin wird die dargestellte und erläuterte Konzeption des Lifelong DNN Algorithmus prototypisch implementiert und die definierten Testfälle werden durchgeführt.

# Aufbau der Evaluierung

In dieser Arbeit wird der L DNN Algorithmus untersucht und sein Potenzial bewertet. Um eine belastbare Aussage über den Algorithmus treffen zu können, müssen Tests definiert werden, welche zur Evaluierung genutzt werden. Für diese Aussage werden Tests definiert und genutzt, die auch für vergleichbare Algorithmen genutzt wurden. Dafür werden öffentlich zugängliche Bilddatensätze genutzt. Zur Bewertung dieser Testfälle werden bekannte Metriken der Objekterkennung/-Klassifizierung genutzt.

## Datensätze

Zur Evaluierung werden öffentlich zugängliche Bilddatensätze genutzt, welche sehr häufig im Bereich der DNNs zur Bestimmung des Potenzials eines Algorithmus genutzt werden. Zur Auswertung der Performanz des Algorithmus wird die Klassifikationsgenauigkeit bewertet. In dieser Arbeit wird der MNIST- und ImageNet-Datensatz zur Evaluierung des inkrementellen und verteilten Klassen-Lernens genutzt. Dabei werden dem Lifelong DNN neue, bisher unbekannte Klassen gezeigt, welche das Netzwerk auf Basis weniger Beispielbilder erlernen muss. Die Aufgabe des Netzwerks ist es, inkrementell diese neuen Klassen zu erlernen ohne dabei alte, bereits bekannte Klassen zu vergessen.

MNIST kann als Standard-Datensatz im Bereich des maschinellen Lernens angesehen werden. In diesem Datensatz sind insgesamt 70.000 handgeschriebene Zahlen von 0 bis 9 in *Grayscale-*Bildern im Format 28x28 gesammelt, aufgeteilt in 60.000 Trainings- und 10.000 Testbilder. Die Aufgabe für das Klassifikator-Netzwerk besteht darin, die Zahlen korrekt zu klassifizieren. Für die konkrete Aufgabenstellung des inkrementellen Klassenlernens wird der sogenannte *Split-MNIST* Datensatz genutzt. Dafür werden jeweils 2 benachbarte Zahlen (z.B. 0/1 und 2/3) zu einer Gruppe zusammengefasst. Diese werden dem Netzwerk gezeigt. Nach einer gewissen Anzahl an Bildern pro Klasse (Wiederholungen) wird die nächste Gruppe dem Netzwerk gezeigt. Nachdem alle Gruppen dem Netzwerk gezeigt wurden, werden Testbilder aller Klassen gezeigt und die Klassifikationsgenauigkeit bestimmt. Dieser Testfall des Split-MNIST Datensatz kann als Grundlagenuntersuchung verstanden werden. Der Datensatz stellt kein allzu komplexes Problem dar, kann jedoch in einem ersten Schritt genutzt werden, um die prinzipielle Funktion eines Ansatzes zu untersuchen und mit anderen Ansätzen zu vergleichen, da es für diesen Datensatz eine Vielzahl an Untersuchungen gibt und somit die Performanz gut mit anderen Algorithmen verglichen werden kann.

Zusätzliches wird der ImageNet-Datensatz für die Evaluierung genutzt. Dieser Datensatz stellt ein komplexes Problem mit über 1 Millionen Bilder von 1.000 unterschiedlichen Klassen dar. Die Bilder sind RGB-Bilder im Format 224x224. Allein die Größe und Farbe des Bildes erschwert die Aufgabe im Vergleich zum MNIST-Datensatz wesentlich. Weiterhin gibt es eine Vielzahl an unterschiedlichen Klassen und eine hohe Varianz zwischen diesen, von mehreren unterschiedlichen Hunderassen über Containerschiffe zu einem Polizeiauto. Auf Basis dieses Datensatzes werden zwei Testfälle definiert. Zunächst ein Testfall, bei dem zehn unterschiedliche Klassen nacheinander inkrementell erlernt werden. Dabei soll das für MNIST gezeigte Verhalten mit wenigen Klassen auf einer komplexeren Aufgabe nachgestellt und generalisiert werden. Zudem wird auf Basis des ImageNet-Datensatzes ein Testfall mit einer großen Anzahl an Klassen definiert. Dafür werden von den 1.000 verfügbaren Klassen 900 genutzt, um das Klassifikator-Netzwerk zu trainieren. Die weiteren 100 Klassen werden inkrementell erlernt. Diese fehlenden 100 Klassen werden zufällig ausgewählt und können von Testfall zu Testfall variieren, um eine generelle Aussage zu erhalten über die Fähigkeit neue Klassen zu erlernen, wenn das Netzwerk bereits eine große Anzahl an Klassen erlernt hat. Zudem wird in diesem Fall durch die hohe Anzahl an vortrainierten Klassen (900) kein allzu großer Einfluss durch die spezielle Auswahl der Klassen erwartet.

Diese genannten Fälle lassen sich auch für das verteilte Lernen nutzen, was später in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** beschrieben wird.

Relevante Daten und Parameter während der Evaluierung sind die Klassifikationsgenauigkeit und die Anzahl an Wiederholungen, wenn neue Klassen einem Netzwerk gezeigt werden. Weitere DNN-typische und einstellbare Parameter werden in einem separaten Parameterfile geschrieben und mit den Ergebnissen für eine mögliche Reproduzierbarkeit gesichert. Für eine aussagekräftige Bewertung sollen mehrere Wiederholungen pro Testfall durchgeführt werden, um die Varianz abschätzen zu können.

## Evaluierungskriterien

Es wird die Klassifikationsgenauigkeit als Kriterium für die Evaluierung genutzt, welche auch als *True Positive* (*TP*) -Rate bezeichnet wird. Diese Genauigkeit gibt an, wie viele Prozent der Testbilder korrekt klassifiziert werden und somit der korrekten Klasse zugeordnet werden können. Für die Bestimmung dieser Genauigkeit werden die in den Datensätzen enthaltenen, bisher für das Netzwerk unbekannten, Test-Bilder genutzt. Es wird die vom Klassifikator-Netzwerk geschätzte Klasse mit der korrekten Klasse des Bildes verglichen und die Anzahl an korrekten Klassifizierungen gezählt. Diese Anzahl in Relation zu der Menge aller Testbildern ergibt die Klassifikationsgenauigkeit (TP-Rate).

|  |  |  |
| --- | --- | --- |
|  |  | (16) |

Zudem wird untersucht, welchen Einfluss die Anzahl an Wiederholungen von Bildern einer neuen Klasse auf die spätere Klassifikationsgenauigkeit hat. Damit soll untersucht werden, wie viele Wiederholungen (Anzahl an Trainingsbilder pro Klasse) notwendig sind, um eine neue Klasse zu erlernen und somit wie schnell das Netzwerk diese neuen Klassen erlernt. Dafür werden die beschriebenen Anwendungsfälle durchgeführt und die Anzahl an Wiederholungen der Bilder einer neuen Klasse variiert. Zum Schluss wird die Klassifikationsgenauigkeit ermittelt. Mit diesen Ergebnissen kann eine Kurve der Klassifikationsgenauigkeit über die Anzahl an Wiederholungen gezeichnet und der Einfluss bewertet werden.

## Evaluierungsfälle

Wie bereits beschrieben werden konkrete Evaluierungsfälle definiert und zur Bewertung genutzt. In allen Fällen wird die Objektklassifizierung auf Basis von Bildern (Grayscale bei MNIST und RGB bei ImageNet) untersucht. Diese Bilder stellen den Eingang der Testfälle dar. Das Kriterium der Klassifikationsgenauigkeit wird für die Auswertung eingesetzt, um das Potenzial des Algorithmus zu bewerten. Die einzelnen Fälle werden im Folgenden beschrieben.

****Split-MNIST****

**Als Ausgangssituation wird ein untrainiertes Klassifikator-Netzwerk (Modul B) eingesetzt. Der MNIST-Datensatz wird in fünf Gruppen mit jeweils zwei Zahlen eingeteilt (0/1, 2/3, 4/5, 6/7, 8/9). Trainingsbilder jeder Gruppe werden dem Netzwerk für eine einstellbare Anzahl an Wiederholungen gezeigt. Nach der eingestellten Anzahl an Wiederholungen wird angenommen, dass das Netzwerk diese Klassen erlernt hat. Diese Prozedur wird dann für die nächste Gruppe wiederholt. Nachdem alle Klassen gezeigt wurden, ist das Netzwerk in der Theorie auf alle Klassen trainiert. Für die Auswertung der Performanz werden die Testbilder des MNIST-Datensatzes (10.000 Bilder gleichverteilt über alle Klassen) dem Netzwerk gezeigt und die Klassifikationsgenauigkeit bestimmt.**

**Ein weiterer Testfall auf diesem Datensatz untersucht die Fähigkeiten des verteilten Lernens. Dabei werden zwei identisch aufgebaute Netzwerke trainiert, jedoch mit unterschiedlichen Klassen. So wird Netzwerk 1 mit den Gruppen 0/1, 2/3 und 4/5 trainiert, während Netzwerk 2 mit den Gruppen 6/7 und 8/9 trainiert wird. Die beiden Netzwerke tauschen nach dem Training ihre Gewichte aus. Durch den Austausch sollen beide Netzwerke die Fähigkeit erhalten, die jeweils anderen Klassen klassifizieren zu können. Somit sollten beide Netzwerke das Wissen besitzen, um den Test-Datensatz (alle Klassen) korrekt zu klassifizieren.**

**Es wird erwartet, dass Ergebnisse ähnlich klassisch trainierten Netzwerken (im Bereich 95-100%) erzielt werden können. Als Referenz dienen in der Literatur vorhandene Resultate auf diesem Datensatz.**

****ImageNet-10****

Das Vorgehen für diesen Testfall ist identisch zu dem bereits beschriebenen Evaluierungsfall für Split-MNIST. Es sind hier jedoch keine Gruppen von zwei Klassen vorhanden, sondern zehn einzelne unterschiedliche Klassen, die kontinuierlich und einzeln vom Netzwerk erlernt werden. Ansonsten ist bis auf die Eingangsdaten (224x224 RGB Bilder von ImageNet statt 28x28 GrayScale Bilder von MNIST) der Anwendungsfall identisch. Es soll in diesem Evaluierungsfall untersucht werden, ob das schnell lernende Klassifikator-Netzwerk in der Lage ist, solche komplexen Aufgaben korrekt zu lösen und sich die Ergebnisse des einfachen MNIST-Datensatzes auch auf komplexeren Datensätzen erzielen lassen. Die finale Auswertung erfolgt auf den Testbildern. ImageNet beinhaltet pro Klasse 50 Testbilder und somit 500 Testbilder für diesen Fall. Für eine vergleichbare Bewertung und Reproduzierbarkeit über mehrere Wiederholungen werden die benutzten Klassen definiert, da bei der geringen Anzahl an Klassen ein hoher Einfluss durch die Auswahl der Klassen erwartet wird. Die Klassen sind im Folgenden, mit dem Index der jeweiligen Klassen in Klammern, aufgelistet: Königspinguin (145), Malteser (Hunderasse – 153), Schneeleopard (289), Passagierflugzeug (404), Zeppelin (405), Containerschiff (510), Fußball (805), Sportauto (817), Sattelzug (867) und Orange (950). Auch hier soll eine weitere Untersuchung hinsichtlich des verteilten Lernens erfolgen. Auf zwei Netzwerken sollen jeweils fünf der genannten Klassen inkrementell erlernt werden und nach dem Training das Wissen ausgetauscht werden. Das Ergebnis sollte theoretisch nicht wesentlich vom zuvor erzielten Ergebnis mit einem Netzwerk abweichen.

Als Referenz werden vorhandene Ergebnisse aus der Literatur herangezogen.

ImageNet

Bei diesem Anwendungsfall wird der gesamte ImageNet-Datensatz mit seinen 1.000 Klassen genutzt. Dafür wird das Klassifikator-Netzwerk zunächst für 900 Klassen vortrainiert. Dies stellt den Ausgangspunkt dieses Evaluierungsfalls dar. Von diesem Punkt an werden die weiteren 100 Klassen kontinuierlich dem Netzwerk hinzugefügt, so dass dieses die neuen Klassen erlernen kann. Dies stellt ein sehr komplexes Problem dar, da sowohl die Bilder komplexe Eingangsdaten sind, zum anderen auch eine sehr hohe Anzahl und Varianz an Klassen (Tiere, Autos, Schiffe…) vorhanden ist. Dieser Fall mit seiner hohen Komplexität wird für die finale Bewertung des Algorithmus genutzt. Auch hier soll eine weitere Untersuchung hinsichtlich des verteilten Lernens erfolgen. Auf zwei Netzwerken sollen jeweils vom selben Startpunkt aus 50 der 100 unbekannten Klassen inkrementell erlernt werden und nach dem Training das Wissen ausgetauscht werden. Das Ergebnis sollte theoretisch nicht wesentlich vom zuvor erzielten Ergebnis mit einem Netzwerk abweichen.

Auf diesen Ergebnissen soll eine generelle Aussage über das Potenzial getroffen werden können, speziell in Bezug auf dem Einsatz dieses Algorithmus in anderen komplexen realen Anwendungen.

# Evaluierung und Ergebnisse

In diesem Kapitel werden einige grundlegende Anmerkungen geführt. Diese werden zentral zu Beginn aufgeführt, um eine bessere Lesbarkeit im weiteren Verlauf zu gewährleisten und um mehrfach auftretende Änderungen nur einmal zu erwähnen.

Für ImageNet-10 wurden Bilder der Dimension 64x64x3 genutzt, da dieser Datensatz bereits lokal in dieser Konfiguration vorhanden war. Eine Nutzung von 224x224 Bildern hätte einen erheblichen Zusatzaufwand bedeutet. Der Test auf dem gesamten ImageNet-Datensatz wird wie in der Evaluierungsspezifikation beschrieben auf Bildern der Dimensionen 224x224x3 durchgeführt haben.

Aufgrund des vortrainierten MobileNet-v2 konnten nur spezielle Eingangsdimensionen für die Bilder genutzt werden. Die kleinste verfügbare Dimension ist dabei 96x96. Deshalb wurden kleinere Bilder (ImageNet-10 und MNIST) auf diese Dimensionen mithilfe der TensorFlow-Funktion *tf.image.resize* vergrößert. Zusätzlich müssen die Bilder im RGB-Format vorliegen. Für ImageNet-Bilder ist dies der Fall. MNIST-Bilder werden mithilfe der TensorFlow-Funktion *tf.image.grayscale\_to\_rgb* umgewandelt. In Abbildung 23 ist ein Bild des MNIST-Datensatzes vor der Bild-Augmentation im Format 28x28x1 zu sehen. In diesem Format liegen die Bilder des Datensatz vor. Abbildung 23 zeigt die Zahl „7“.

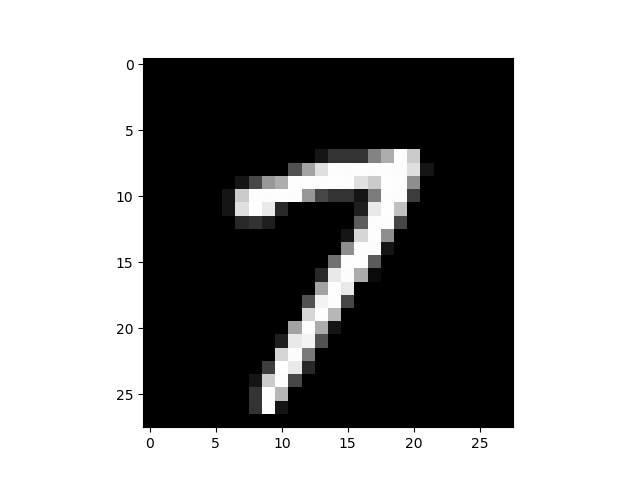


Abbildung 23: MNIST-Bild vor Bild-Augmentation

Abbildung 24 zeigt ein Bild des MNIST-Datensatzes nach der zuvor beschriebenen Bild-Augmentation. Es besitzt nun das Format 96x96x3. Jedoch ist zu sehen, dass das Bild in seiner Grundstruktur nicht wesentlich verändert wurde, wodurch durch diese Bild-Augmentation kein großer Einfluss auf Klassifikationsgenauigkeit erwartet wird. In diesem Beispielbild ist die Zahl „8“ zu sehen.

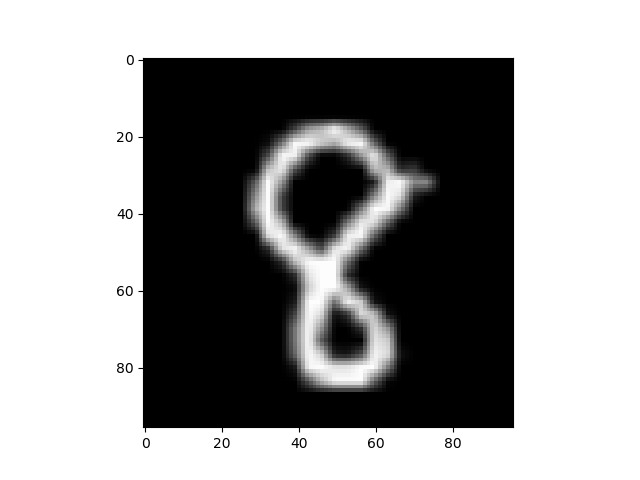


Abbildung 24: MNIST-Bild nach Augmentation

Zusätzlich wird die Bezeichnung des gesamten ImageNet-Datensatzes genauer definiert. Es wird der Datensatz der *ImageNet Large Scale Visual Recognition Challenge* (ILSVRC) aus dem Jahr 2012 genutzt [47]. Als Test-Daten werden wie in der Literatur und für vergleichbare Modelle üblich die frei verfügbaren 50 Validationsbilder pro Klasse genutzt. In dem genutzten Datensatz gibt es für die 1000 Klassen insgesamt 1.281.167 Trainingsbilder. Die Anzahl an Trainingsbilder pro Klasse schwankt dabei zwischen 732 und 1300. Mit 50 Validationsbildern (hier später als Test-Bilder genutzt und bezeichnet) pro Klasse sind 50.000 Validationsbilder vorhanden. Weitere Informationen über die unterschiedlichen Klassen können in [47] nachgelesen werden.

## Hyperparameter-Optimierung Modul B

Neuronale Netzwerke besitzen eine Vielzahl an Hyperparametern, welche abhängig vom konkreten Anwendungsfall und den vorliegenden Daten unterschiedlich eingestellt werden können und müssen für eine optimale Performanz des Netzwerkes. Um eine möglichst optimale Parametrierung des inkrementellen Klassifikators in Modul B zu erhalten, wurden die relevanten Parameter identifiziert und mithilfe einer Gitter-Suche (*Grid Search*) die optimalen Werte für die folgenden Evaluierungsfälle zu finden. Als relevante Parameter des FuzzyARTMAP-Netzwerkes wurden die Lernrate und der Vigilance-Parameter identifiziert, da diese das Training des Netzwerkes und damit am Ende die Performanz im Testfall beeinflussen. Details zu den beiden Modell-Parametern sind in der Konzeption zu finden.

Die in der Evaluierungsspezifikation beschriebenen Fälle des kontinuierlichen Lernens auf einem Endgerät für Split-MNIST und ImageNet-10 werden genutzt, um die oben beschriebenen Hyperparameter zu optimieren und deren Einfluss zu untersuchen. Diese beiden Datensätze erlauben es aufgrund ihres begrenzten Umfangs (lediglich 10 Klassen) viele Tests in kurzer Zeit durchzuführen, was für die Gitter-Suche relevant ist, da dort viele Tests für eine Abdeckung des Gitters erforderlich sind.

Für die Hyperparameter-Optimierung wird eine zwei-dimensionale Gitter-Suche mit den Parametern und durchgeführt. Dafür werden diese beiden Parameter jeweils im Bereich in 0,1-er Schritten erhöht. Es werden 5 Wiederholungen pro mögliche Kombination durchgeführt, um eine statistische Aussagekraft zu erhalten. Das Vorgehen resultiert in jeweils 500 Tests für Split-MNIST und ImageNet-10. Die weiteren Parameter werden auf fixe Werte eingestellt, welche im Folgenden aufgelistet sind:

* modul\_b\_epsilon = 0,001
* modul\_b\_s = 1,05
* train\_img\_per\_class = 20
* test\_img\_per\_class = 100

Auf der Basis der erzielten Ergebnisse werden und ausgewählt.

Zu erwähnen ist, dass die Gruppen für Split-MNIST in einer festen Reihenfolge gezogen wurden (wie in der Evaluierungsspezifikation beschrieben). Bei ImageNet-10 wird die Reihenfolge der Klassen zufällig bestimmt, um eine zusätzliche Varianz der Trainingsdaten mit einzubeziehen.

Für beide Datensätze werden in jeder Wiederholung zufällig die benötigte Anzahl (20) an Trainingsbilder aus dem größeren Trainingsdatensatz gezogen. Die ermittelte Genauigkeit wird auf Validationsdaten aus dem Trainings-Datensatz bestimmt. Diese Bilder werden nicht für das Training verwendet. Durch die Wiederholung und das zufällige Ziehen der Trainings- und Validations-Samples findet eine Kreuz-Validation der Ergebnisse statt. Die Test-Datensätze werden dann im späteren Verlauf der Arbeit zur finalen Performanz-Bewertung eingesetzt.

Zur Umsetzung des Tests müssen lediglich die Parameter gesetzt werden und die korrekten Parameter in den jeweiligen *for-*Schleifen eingesetzt werden. Dann kann der beschriebene SW-Prototyp ausgeführt werden und die *Main*-Funktion iteriert automatisch über alle Testfälle und sichert die Ergebnisse in den passenden Ordnern ab.

Nachdem alle Tests durchlaufen sind, können mithilfe des zusätzlichen Auswerte-Skripts (*Evaluation\_Results.py*) die gewünschten Metriken und Graphen für die verschiedenen Fälle erstellt werden.

In diesem Kapitel werden die Ergebnisse für Split-MNIST und ImageNet-10 bewertet.

Es wird erwartet, dass für sehr kleine und große Werte von (Werte nahe 0 und 1) schlechte Ergebnisse erzielt werden, da bei diesen Fällen kaum ein Lernen stattfindet. Bei werden neue Trainingsdaten nicht genutzt und bei wird lediglich das neue Trainingssample genutzt und die alte Repräsentation damit überschrieben. Hier muss ein Wert gefunden werden, der es erlaubt altes, vorhandenes Wissen mit neuen Samples zu verbinden um eine möglichst ideale und generalisierte Repräsentation dieser Klasse zu bilden.

Bei wird erwartet, dass ab einem gewissen Wert keine Änderung mehr zu erkennen ist, da die Ähnlichkeit zwischen zwei Samples einer Klasse selten nahe 1 liegt. Dieser Schwellwert für wird für die unterschiedlichen Datensätze unterschiedlich erwartet. Ab diesem Schwellwert kann gesagt werden, dass jedes Sample, das im Training gesehen wird, als neue Repräsentation angelegt wird. Dies erfordert einen hohen Speicherbedarf. Zudem sind die erhaltenen Repräsentationen nicht generalisiert, wodurch auf späteren, abweichenden Test-Daten keine guten Generalisierungsfähigkeiten erwartet werden. Deshalb muss ein Wert für unterhalb dieser Schwelle gefunden werden. Ein zu kleiner Wert für führt dazu, dass die einzelnen Klassen durch sehr wenige (im Extremfall durch eine) Repräsentationen dargestellt werden. Je nach Klasse kann das positiv sein (wenn alle Samples der Klasse sehr ähnlich aussehen). Im Allgemeinen ist das aber nicht wünschenswert, da dadurch abweichende Samples der Klasse (zum Beispiel eine verdrehte Zahl) nicht gut erkannt werden können. Deshalb muss für ein guter Mittelwert zwischen zu vielen und zu wenigen Repräsentationen gewählt werden.

In Abbildung 25 sind die Ergebnisse der beschriebenen Gitter-Sucher zur Hyperparameter-Optimierung von Modul B auf Basis des Split-MNIST Datensatzes dargestellt. Entlang der x-Achse sind die unterschiedlichen Werte von zu sehen und entlang der y-Achse sind die Werte für aufgetragen. In den jeweiligen Feldern ist der Mittelwert der Klassifikationsgenauigkeit aus den fünf Wiederholungen für diese Parameterkombination eingetragen.



Abbildung 25: Ergebnisse der Gitter-Suche für und auf Basis des Split-MNIST Datensatzes

In Abbildung 26 sind die Ergebnisse für dieselben Testfälle auf Basis des ImageNet-10 Datensatzes dargestellt. Die Darstellungsart ist dabei identisch wie bereits für Abbildung 25 beschrieben.

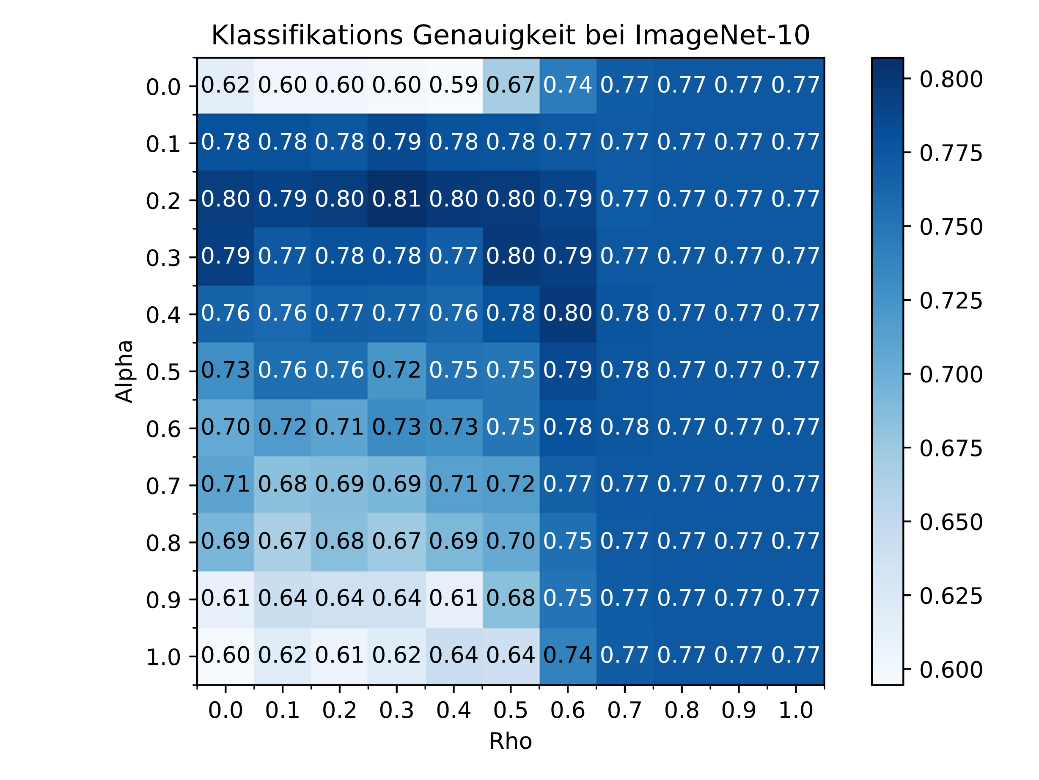


Abbildung 26: Ergebnisse der Gitter-Sucher für und auf Basis des ImageNet-10 Datensatzes

Die Ergebnisse werden für beide Parameter getrennt bewertet werden, da es keine relevante Korrelation der beiden Parameter gibt.

Zunächst werden die Ergebnisse für den Parameter bewertet. Hier ist das erwartete Verhalten zu erkennen. Bei beiden Datensätzen sind für hohe Werte von (>0,8) schlechte Ergebnisse zu sehen, da in diesem Fall lediglich die neuen Daten verwendet werden, um die Repräsentation zu bilden. Bei sind ebenfalls schlechte Ergebnisse zu beobachten, weil nur das erste gesehene Sample genutzt wird, um die Repräsentation zu bilden. Anhand der in Abbildung 25 und Abbildung 26 dargestellten Ergebnisse lassen sich für und die besten Ergebnisse erzielen. Für Split-MNIST variieren die besten Ergebnisse zwischen diesen beiden Werten von , abhängig vom Wert für . Bei ImageNet-10 können jedoch die besten Ergebnisse mit erzielt werden, weshalb dieser Wert im weiteren Verlauf der Arbeit genutzt wird.

Der Parameter ist maßgeblich dafür relevant, wie viele Repräsentationen angelegt werden. Damit beeinflusst direkt, wie groß der Speicherbedarf des FuzzyARTMAP-Netzwerks ist. Deshalb muss bei diesem Parameter auf einen Trade-Off zwischen Performanz und Speicherbedarf geachtet werden. Das erwartete Verhalten, bei dem ab einem gewissen Schwellwert kaum Veränderung in der Klassifikationsgenauigkeit beobachtet werden kann, kann durch die Versuche bestätigt werden. Bei Split-MNIST ist dieser Schwellwert bei ca. 0,9 zu sehen, während bei ImageNet-10 dieser bereits bei 0,7 zu beobachten ist. Dieser Unterschied kann mit der Komplexität der Bilder erklärt werden. Aufgrund der komplexen Bilder von ImageNet-10 sind die Ähnlichkeiten der einzelnen Bilder zueinander geringer, wodurch bereits bei niedrigeren Werten von nahezu jedes Trainingssample als Repräsentation angelegt wird. Bei Split-MNIST sind die besten Ergebnisse mit den Werten 0,9 und 1 zu beobachten. Das sind die Fälle, bei denen jedes Trainingssample als Repräsentation abgelegt wird. Bei ImageNet-10 sind die besten Ergebnisse für zu sehen.

Für Split-MNIST zeigt Abbildung 25 das erwartete Ergebnis für . Es wird die beste Klassifikationsgenauigkeit (87%) erreicht, da sehr viele Repräsentationen pro Klasse angelegt werden. Für ImageNet-10 ist dieses Verhalten nicht zu sehen. Dort werden die besten Ergebnisse (80-81%) für erreicht. Bei ist die Performanz wie erwartet stabil auf einem Niveau, allerdings nur bei ca. 77% Klassifikationsgenauigkeit. Ein Grund dafür könnte in den Bildern des ImageNet-Datensatzes liegen. Die Objekte sind in realer Umgebung zu sehen, und der Hintergrund/die Umgebung ist nicht schwarz wie bei MNIST. Dadurch kann es vorkommen, dass der Feature-Extrahierer (Modul A) unrelevante Features aus dem Hintergrund extrahiert (zum Beispiel starkes Vorkommen der Farbe Blau im Hintergrund bei Flugzeugen aufgrund des Himmels). Diese extrahierten Features geben jedoch keine Information über das Objekt. So können Features von Flugzeugen gleich (sehr ähnlich) denen von Vögeln sein, wenn beide im Himmel mit blauem Hintergrund abgebildet sind. Deshalb können sich einzelne, nicht generalisierte Repräsentationen den Validationsbildern von anderen Klassen ähneln, da einzelne Bilder der unterschiedlichen Klassen aufgrund nicht relevanter Features einen ähnlichen Feature-Vektor besitzen können.

Die genannten Schwellen spiegeln sich direkt im Speicherbedarf von Modul B wider. Ab dem genannten Schwellwert steigt der Speicherbedarf stark an, da viele Repräsentationen angelegt werden. Der mittlere Speicherbedarf von Modul B für Split-MNIST und ImageNet-10 ist in Abbildung 27 und Abbildung 28 graphisch dargestellt.

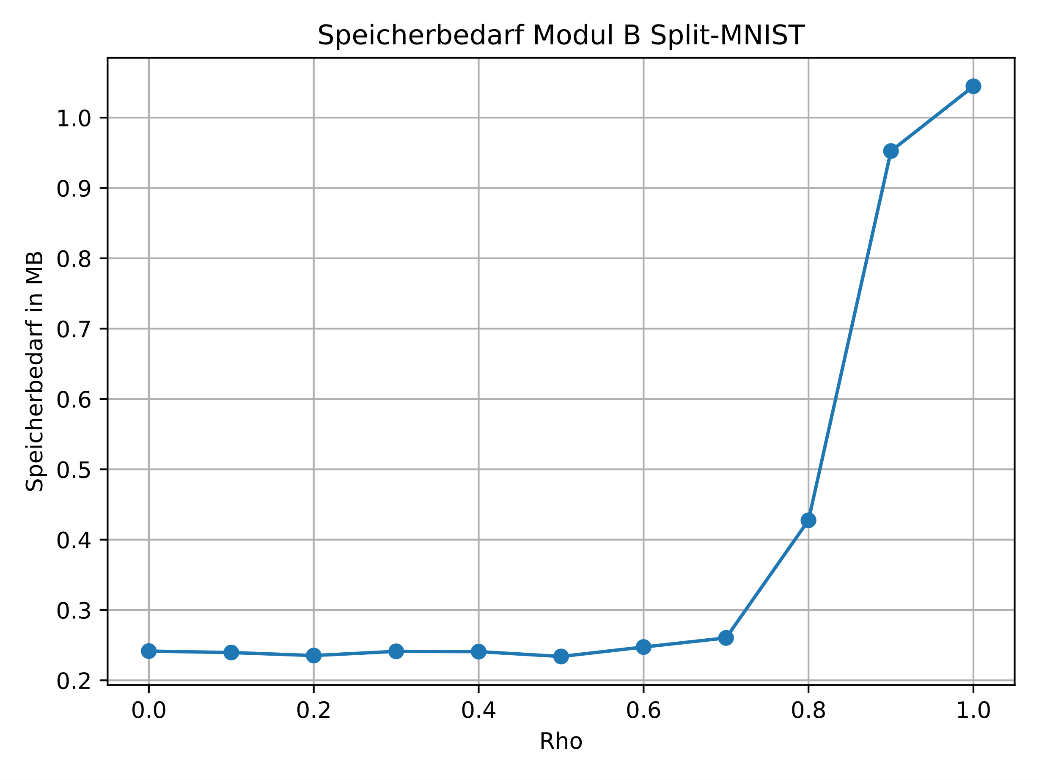


Abbildung 27: Speicherbedarf von Modul B in Abhängigkeit von für Split-MNIST

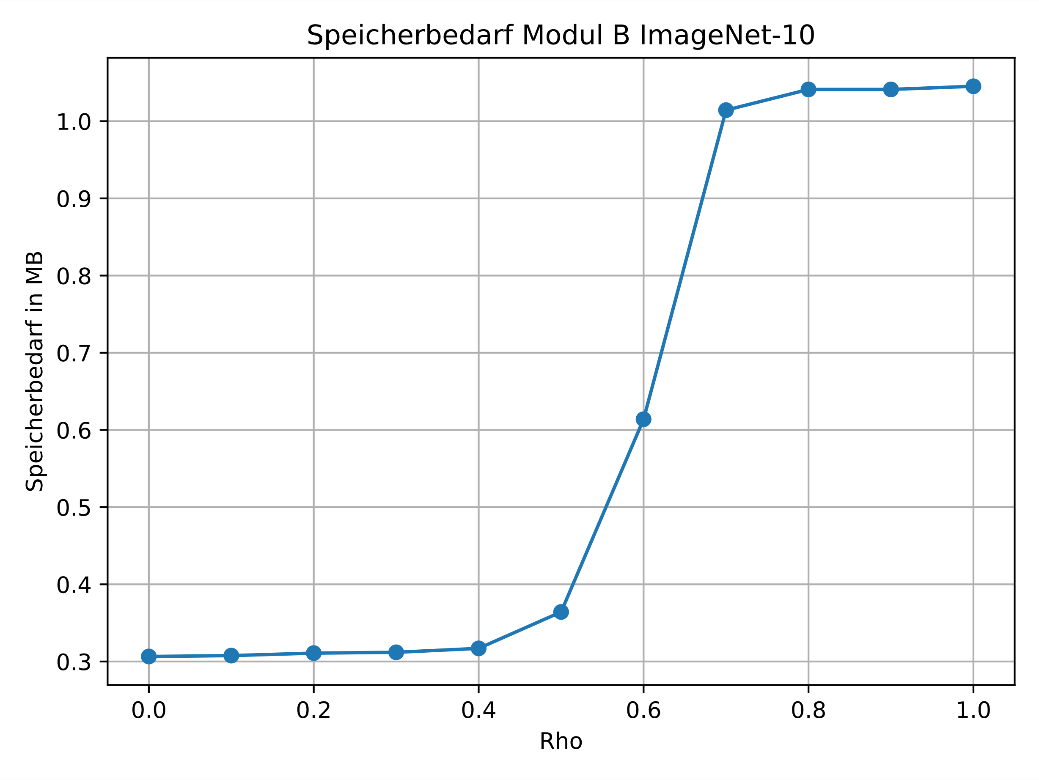


Abbildung 28: Speicherbedarf von Modul B in Abhängigkeit von für ImageNet-10

In diesen Abbildungen ist zu sehen, dass der Speicherbedarf ab dem Schwellwert (~0,9 für Split-MNIST und ~0,7 für ImageNet-10) auf das 3- bist 4-fache des davor benötigten Speicherbedarfs ansteigt.

Aufgrund der geringen Anzahl an Trainingsbildern (20 pro Klasse) ist der Speicherbedarf mit ca. 1MB in diesen Beispielen immer noch gering. Bei späteren Anwendungen mit mehr Klassen oder Trainingsbildern kann der Speicherbedarf jedoch schnell sehr groß werden. Auf Basis dieser Ergebnisse hinsichtlich Genauigkeit und Speicherbedarf wird für der Wert 0,5 gewählt. Mit diesem Parameterwert können auf beiden Datensätzen eine gute Klassifikationsgenauigkeit erzielt werden und der Speicherbedarf ist mit ca. 250 KB für Split-MNIST und ca. 350 KB für ImageNet-10 gering. Für weitere komplexere Anwendungen (z.B. gesamter ImageNet-Datensatz) wird der Speicherbedarf mit dieser Parametrierung in einem akzeptablen Bereich erwartet.

## Einfluss der Anzahl von Trainingsdaten

Schnell lernende inkrementelle Klassifikatoren sollen auf Basis von wenigen Beispieldaten einer Klasse diese erlernen können. Ein wichtiges Indiz ist dabei die Klassifikationsgenauigkeit in Abhängigkeit der gesehenen Anzahl an Samples pro Klasse. Damit kann untersucht werden, ab wie vielen Trainingssamples ein Maximum an Genauigkeit erreicht werden kann und wie sich der Performanz-Gewinn durch eine höhere Anzahl an Trainingsbilder verhält.

Wie in den Kriterien der Evaluierungsspezifikation dargestellt, wird dieser Test genutzt, um eine Aussage über die Fähigkeit des Algorithmus zu erhalten, schnell neue Klassen zu erlernen.

Es werden die zuvor ermittelten Hyperparameter von Modul B verwendet. Mit diesen Parametern wird als weitere Untersuchung die Anzahl an Trainingsbildern variiert. Die Anzahl der Trainingsbilder wird dabei auf folgende Werte gesetzt: . Es werden pro Parameterwert 5 Wiederholungen durchgeführt, um einen aussagekräftigen statistischen Mittelwert und die Standardabweichung bilden zu können. Die weiteren einstellbaren Parameter sowie der Ablauf sind wie in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** beschrieben.

Es wird erwartet, dass mit mehr Trainingsbildern pro Klasse bessere Ergebnisse erzielt werden können, da mehr und besser generalisierte Repräsentationen für die einzelnen Klassen angelegt werden können. Mit steigender Anzahl an Trainingsbildern pro Klasse wird vermutet, dass die Varianz der Klassifikationsgenauigkeit abnimmt und damit stabilere Ergebnisse erzielt werden können. Die Annahme ist, dass bei wenigen Trainingsbildern die spätere Klassifikationsgenauigkeit stark von der Auswahl dieser wenigen Trainingsbilder abhängig ist. Bei steigender Anzahl an Trainingsbilder sinkt die Abhängigkeit von den einzelnen Trainingsbilder.

Zudem ist die Erwartung, dass der Speicherbedarf mit der Anzahl an Trainingsbildern steigt, da mehr Repräsentationen durch die höhere Zahl an gesehenen Trainingsdaten angelegt werden.

Die Ergebnisse für die Klassifikationsgenauigkeit werden in einem Balkendiagramm dargestellt. Die schwarzen Linien stellen dabei die Standardabweichung um den Mittelwert dar. Aufgrund der großen Unterschiede zwischen den einzelnen Werten für die Anzahl an Trainingsbilder wird die x-Achse in logarithmischer Skala dargestellt.

In Abbildung 29 ist die Klassifikationsgenauigkeit für Split-MNIST dargestellt.

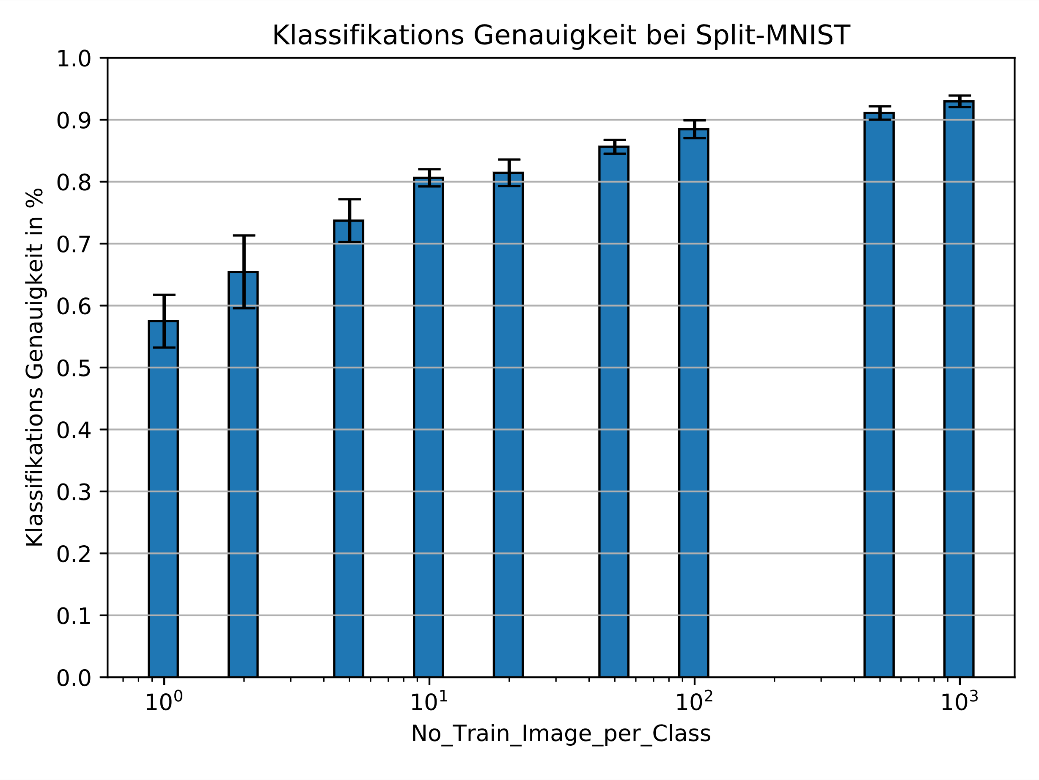


Abbildung 29: Klassifikationsgenauigkeit über die Anzahl an Trainingsbildern Split-MNIST

Abbildung 30 stellt die Klassifikationsgenauigkeit über die Anzahl an Trainingsbildern für ImageNet-10 dar.

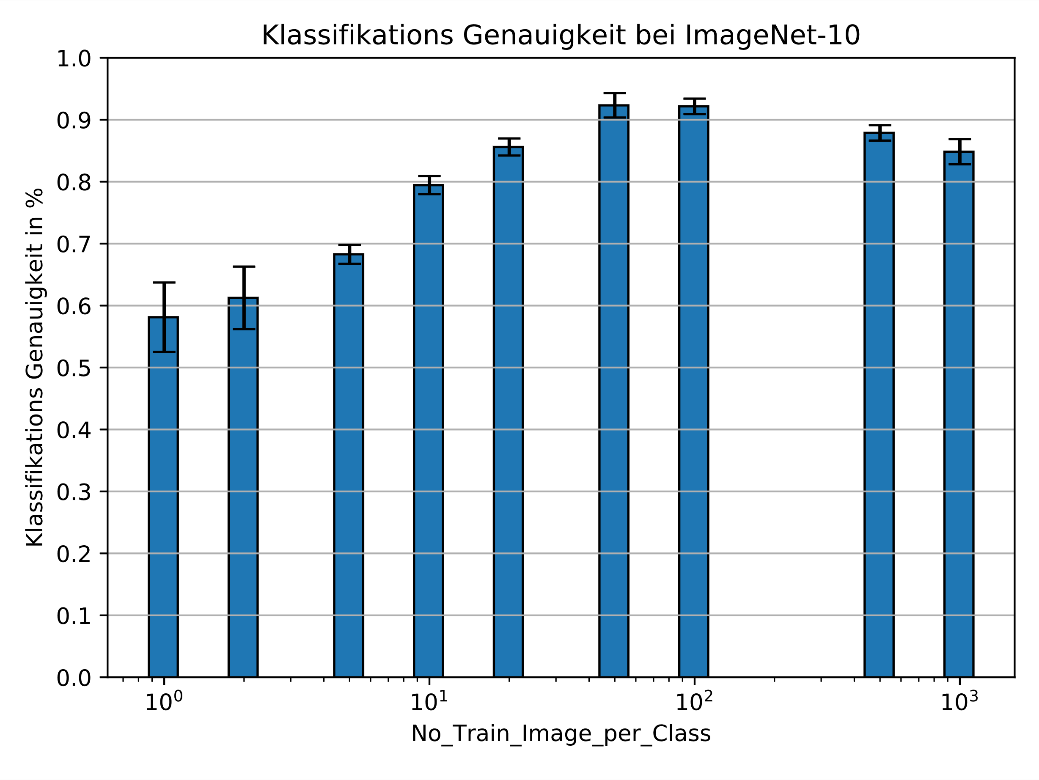


Abbildung 30: Klassifikationsgenauigkeit über die Anzahl an Trainingsbildern ImageNet-10

Zusätzlich wird der mittlere Speicherbedarf von Modul B für die jeweiligen Datensätze in Abhängigkeit von der Anzahl an Trainingsbildern in Abbildung 31 für Split-MNIST und in Abbildung 32 für ImageNet-10 dargestellt.

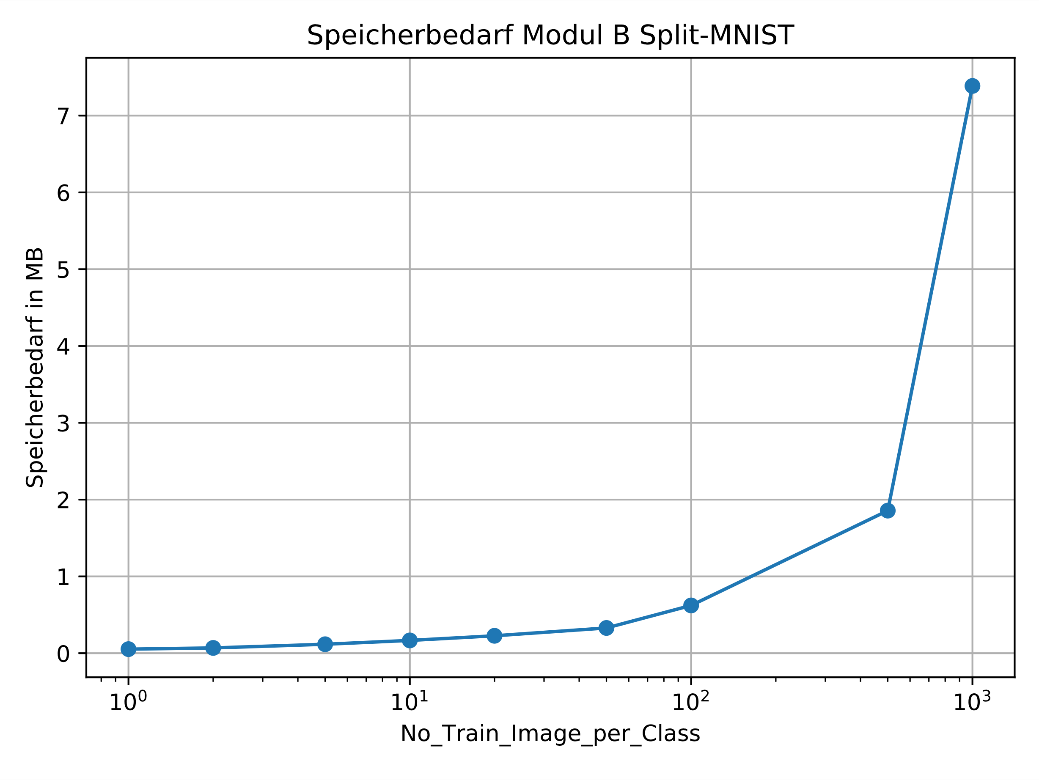


Abbildung 31: Speicherbedarf Modul B über die Anzahl an Trainingsbildern Split-MNIST

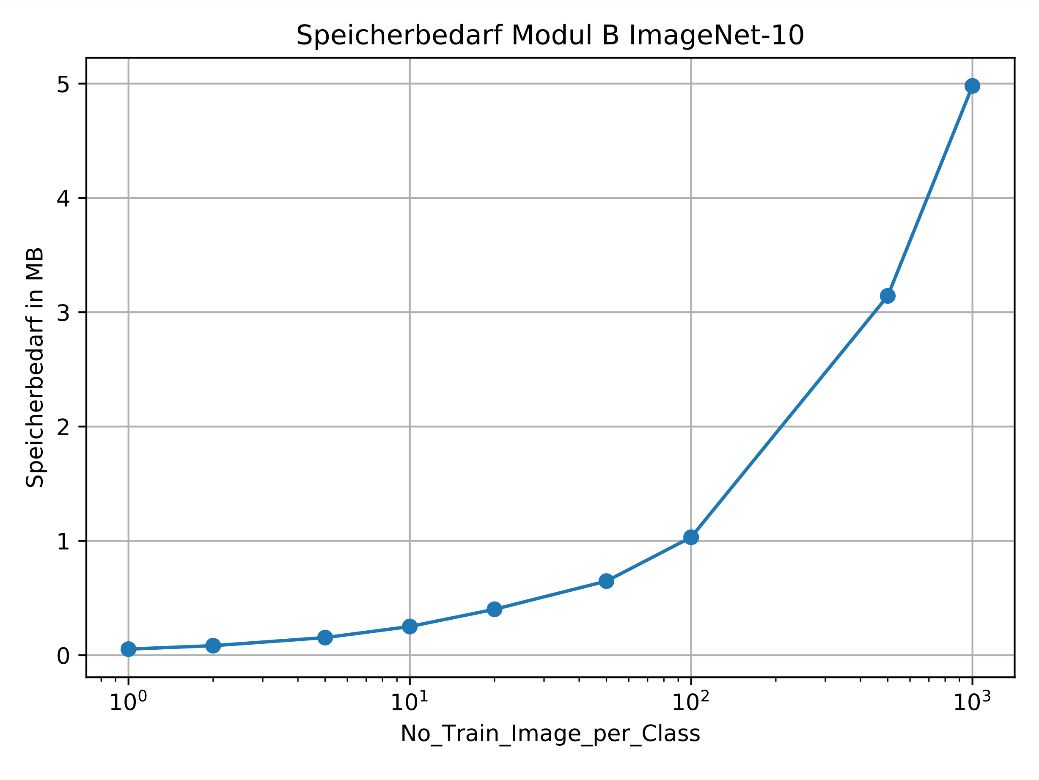


Abbildung 32: Speicherbedarf Modul B über die Anzahl an Trainingsbildern ImageNet-10

Die Auswertung der gezeigten Ergebnisse findet im folgenden Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.** statt.

Die Annahme, dass mit einer geringen Anzahl an Trainingsbildern eine hohe Varianz auftritt, kann auf Basis der erzielten Ergebnisse bestätigt werden. Für Split-MNIST (Abbildung 29) beträgt die Standardabweichung bei einem beziehungsweise zwei Trainingsbildern pro Klasse 4,3 und 5,9 Prozentpunkte. Mit 500 und 1000 Trainingsbildern pro Klasse beträgt die errechnete Standardabweichung lediglich 1,1 und 0,9 Prozentpunkte.

Bei ImageNet-10 ist ebenfalls eine höhere Standardabweichung bei einer geringen Anzahl Trainingsbildern zu sehen mit 5,6 und 5,1 Prozentpunkten bei einem und zwei Trainingsbildern pro Klasse. Die geringste Abweichung ist für ImageNet-10 mit jeweils 1,2 Prozentpunkten bei 100 und 500 Trainingsbildern pro Klasse zu finden.

Wenn die Klassifikationsgenauigkeit an sich betrachtet wird, kann für Split-MNIST gesagt werden, dass mit mehr Trainingsbildern pro Klasse die Genauigkeit besser wird. Bei 1000 Trainingsbildern pro Klasse wird im Mittel eine Klassifikationsgenauigkeit von 92,96% bei einer Standardabweichung von +/-0,94 erreicht. Mit 500 Trainingsbildern pro Klasse kann ebenfalls bereits eine gute Klassifikationsgenauigkeit von 91,08% +/- 1,1 erreicht werden.

Da aber zusätzlich der Speicherbedarf in Abbildung 31 in Betracht gezogen wird, werden im weiteren Verlauf der Arbeit 500 Trainingsbilder pro Klasse für Split-MNIST genutzt. Der Speicherbedarf steigt zwischen 500 und 1000 Trainingsbildern pro Klasse von ca. 1,9 MB auf ca. 7,2 MB an. Da Speicherbedarf in dieser Arbeit eine Rolle spielt, kann die leicht geringere Genauigkeit (ca. 1 Prozentpunkt) akzeptiert werden, wenn dafür weniger als ein Drittel an Speicher benötigt wird.

Für ImageNet-10 lässt sich ein anderes Verhalten der Klassifikationsgenauigkeit beobachten. Die Genauigkeit steigt zunächst bis 100 Trainingsbildern pro Klasse an, jedoch fällt die Genauigkeit im Gegensatz zu Split-MNIST daraufhin wieder ab. Ein möglicher Grund könnte der bereits beschriebene Fall von zu vielen Repräsentation sein (siehe die Auswertung des Parameters in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**). Die beste Klassifikationsgenauigkeit lässt sich mit 50 und 100 Trainingsbildern pro Klasse erzielen, mit 92,31% +/- 1,9 und 92,16% +/- 1,2. Aufgrund der minimal geringeren Varianz und damit dem besseren „Worst-Case“ Ergebnis (90,41% vs. 90,96%) werden 100 Trainingsbilder pro Klasse für die weiteren Untersuchungen mit dem ImageNet-10 Datensatz genutzt. Auch der Speicherbedarf ist für 100 Trainingsbildern pro Klasse mit ca. 1 MB noch akzeptabel (Abbildung 32).

Insgesamt hat die Anzahl an Trainingsbildern pro Klasse einen, wie erwartet, direkten Einfluss auf die spätere Klassifikationsgenauigkeit. Bereits mit wenigen Trainingsbildern pro Klasse (z.B. 10) können jedoch akzeptable Klassifikationsgenauigkeiten von ca. 80% für die genutzten Validationsdaten von Split-MNIST und ImageNet-10 erreicht werden. Generell kann gesagt werden, dass mit steigender Anzahl an Trainingsbilder die Klassifikationsgenauigkeit ebenso wie der Speicherbedarf des inkrementellen Klassifikator zunimmt. Je nach Anwendungsfall kann eine geringere Genauigkeit infolge von weniger Trainingsdaten akzeptiert werden, wenn z.B. die Erzeugung von Trainingsdaten sehr kosten- und zeitaufwändig ist.

Mit diesem Testfall kann gezeigt werden, dass der hier untersuchte Algorithmus für spätere Anwendungen, bei denen wenigen Daten pro Klasse verfügbar sind, geeignet ist, da er bereits mit wenigen Trainingsbildern pro Klasse gute Ergebnisse erzielen kann.

## Finale Ergebnisse

Für eine abschließende Bewertung und Einordnung des Potenzials des L DNN Algorithmus werden auf Basis der zuvor untersuchten Hyperparameter finale Tests für das kontinuierliche Lernen durchgeführt. Dabei wird eine größere Anzahl an Wiederholungen mit festen Parametern durchgeführt. Zudem werden die finalen Ergebnisse auf Basis der Testdaten der Datensätze ermittelt, nachdem zuvor für die Untersuchungen der Hyperparameter eine Kreuzvalidation mithilfe von Trainings- und Validationsdaten durchgeführt wurde.

Die in Kapitel 4 der Evaluierungsspezifikation genannten Testfälle werden nun durchgeführt. Für die Erstellung der folgenden Metriken werden Daten genutzt, die das Netzwerk bisher noch nicht gesehen hat. Dadurch kann eine Optimierung und *Overfitting* des Netzwerks auf Testdaten verhindert werden.

### Kontinuierliches Lernen

Es werden die Testfälle des kontinuierlichen Lernens auf einem Gerät durchgeführt. Die Parameter werden auf Basis der vorherigen Ergebnisse ausgewählt und sind im Folgenden nochmals aufgelistet. Als Testdaten werden alle verfügbaren Testbilder der jeweiligen Datensätze genutzt.

* modul\_b\_epsilon = 0,001
* modul\_b\_s = 1,05
* modul\_b\_alpha = 0,2
* modul\_b\_rho = 0,5
* train\_img\_per\_class = 100 (ImageNet-10), 500 (Split-MNIST)
* test\_img\_per\_class = 50 (ImageNet-10), 1000 (Split-MNIST)

Es werden 10 Wiederholungen pro Datensatz durchgeführt.

In diesem Abschnitt werden die Ergebnisse dargestellt. Dafür wird für Split-MNIST eine Tabelle mit Ergebnissen anderer *Continual Learning*-Verfahren aus der Literatur sowie aktueller Ergebnisse mit traditionellen Deep Learning Ansätzen, hier einem Multy-Layer Perceptron (MLP) angelegt.

Für ImageNet-10 sind keine weiteren Ergebnisse von *Continual Learning*-Verfahren bekannt. Dieser Datensatz diente lediglich der Überprüfung des Potenzials auf komplexeren Eingangsdaten. Für einen Vergleich zu anderen Verfahren werden Test auf dem gesamten ImageNet-Datensatz durchgeführt (siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**).

In Tabelle 10 sind die Ergebnisse für den Split-MNIST Datensatz dargestellt. Die ersten beiden Zeilen sind dabei der hier untersuchte Algorithmus. *L DNN Algorithmus inkrementell* ist der wie in der Evaluierungsprozedur beschriebene inkrementelle Algorithmus. *L DNN Algorithmus gesamt* ist dieselbe Architektur mit derselben Parametrierung, jedoch werden die Trainingsbilder aller Klassen gemeinsam in einem großen Batch trainiert und nicht inkrementell. Bei den weiteren Algorithmen ist angegeben, von welcher Quelle die genannte Klassifikationsgenauigkeit stammt. Die Ergebnisse gelten für den Fall des inkrementellen Klassen Lernens.

Tabelle 10: Klassifikationsgenauigkeit verschiedener Algorithmen auf Split-MNIST

|  |  |
| --- | --- |
| Algorithmus | Klassifikationsgenauigkeit in % |
| L DNN Algorithmus gesamt | 90,66 +/- 0,32 |
| L DNN Algorithmus inkrementell | 86,94 +/- 1,29 |
| Deep Generativ Replay (DGR) [13] | 91,24 +/- 0,33 |
| Elastic Weight Consolidation (EWC) [48] | 19,90 +/- 0,05 |
| Synaptic Intelligence (SI) [48] | 20,04 +/- 0,08 |
| Multi-Layer Perceptron (MLP) – inkrementell trainiert [48] | 19,90 +/- 0,02 |
| MLP – offline trainiert [48] | 97,93 +/- 0,04 |

EWC und SI stellen typische Methoden des kontinuierlichen Lernens dar. Diese Methoden speichern keine Trainingsdaten und nutzen keine gespeicherten Repräsentationen zum Training. Diese Abspeicherung und Verwendung der gespeicherten Daten im weiteren Trainingsverlauf wird in der Literatur *Replay* oder *Rehearsal* genannt. Deep Generative Replay (DGR) nutzt diese Methode, in dem es komprimierte Repräsentationen der Trainingsdaten abspeichert. Wenn neue Klassen hinzukommen, werden aus den gespeicherten Komprimierungen der alten Klassen sowie mithilfe eines erlernten generativen Moduls Trainingsbilder dieser Klassen erzeugt (Generative) und in die neuen Trainingsdaten eingebracht. Das *inkrementell trainierte MLP* kann als untere Grenze gesehen werden, da hier *Catastrophic Forgetting* aufgrund des *Backpropagation*-Algorithmus auftritt. Das *offline trainierte MLP* wurde mit allen Klassen offline trainiert, und kann als obere Grenze angesehen werden.

Für ImageNet-10 wird eine gemittelte Klassifikationsgenauigkeit von 76,4% +/-1,2 beim inkrementellen Erlernen erreicht. Vergleichbare Ergebnisse für diesen Anwendungsfall sind in der Literatur nicht zu finden. Als Referenz wird das Training der Architektur mit den Trainingsbildern aller Klassen herangezogen, wie für den *L DNN Algorithmus gesamt* bei Split-MNIST beschrieben. Mit diesem Training wird eine Klassifikationsgenauigkeit von 76,08% +/- 1,67 erreicht.

Für Split-MNIST können die Ergebnisse mit anderen *Continual Learning* Algorithmen verglichen werden, da es viele Untersuchungen auf Basis dieses Datensatzes gibt. Im Vergleich zu den klassischen Methoden wie EWC und SI kann der L DNN Algorithmus deutlich bessere Ergebnisse für das hier untersuchte inkrementelle Klassen Lernen erzielen.

Algorithmen, die mit generativen Methoden arbeiten (wie DGR), erreichen eine bessere Klassifikationsgenauigkeit für diesen Anwendungsfall. Allerdings besitzen sie auch eine erhöhte Komplexität während des Trainings. Denn bei diesen Modellen muss zusätzlich zu dem inkrementellen Klassifikator ein generatives Modell trainiert werden, welches ausgewählte Trainingsdaten komprimiert und aus den komprimierten Darstellungen wiederherstellt (z.B. mithilfe eines *Variational Auto-Encoder*). Zudem müssen diese komprimierten Darstellungen abgespeichert werden. All diese Punkte ermöglichen generativen Modellen eine bessere Klassifikationsgenauigkeit, jedoch sind diese Modelle aus den genannten Gründen (noch) nicht für den Einsatz auf einem mobilen Endgerät geeignet, was in dieser Arbeit ein wichtiger Auswahlpunkt für den Algorithmus war. Insgesamt ist festzuhalten, dass eine Genauigkeit von ca. 87% auf Split-MNIST ein sehr gutes Resultat für das inkrementelle Klassenlernen ohne Replay/Rehearsal ist. Wenn lediglich Algorithmen ohne Rehearsal betrachtet werden, konnte in der Literatur keine bessere Klassifikationsgenauigkeit auf diesem Datensatz für das inkrementelle Klassenlernen gefunden werden. Als zusätzliche Referenz kann der *L DNN Algorithmus gesamt* gesehen werden. Dabei ist zu sehen, dass durch das inkrementelle Erlernen der Klassen ca. 3,5 Prozentpunkte Klassifikationsgenauigkeit verloren geht bei Split-MNIST.

Die Ergebnisse für ImageNet-10 können nicht mit anderen Algorithmen verglichen werden, jedoch kann damit geprüft werden, ob der Algorithmus auch auf komplexeren Eingangsdaten (64x64 RGB-Bilder mit komplexen Klassen) funktioniert, bevor ein großer und aufwändiger Test auf dem gesamten ImageNet-Datensatz durchgeführt wird. Mit einer finalen mittleren Klassifikationsgenauigkeit von 76,4% kann gesagt werden, dass der Algorithmus auch komplexere Klassen und Eingangsdaten korrekt klassifizieren und inkrementell erlernen kann. Auch wird beim inkrementellen Klassenlernen eine nahezu identische Genauigkeit (sogar minimal besser) wie beim Training der Architektur mit allen Trainingsbildern der Klassen (*L DNN Algorithmus gesamt*) erreicht.

### Verteiltes Lernen

Die Testfälle des verteilten Lernens werden auf zwei Geräten durchgeführt. Die Parameter werden auf Basis der vorherigen Testfälle ausgewählt und sind im Folgenden nochmals aufgelistet. Als Testdaten werden alle verfügbaren Testbilder der jeweiligen Datensätze genutzt.

* modul\_b\_epsilon = 0,001
* modul\_b\_s = 1,05
* modul\_b\_alpha = 0,2
* modul\_b\_rho = 0,5
* train\_img\_per\_class = 100 (ImageNet-10), 500 (Split-MNIST)
* test\_img\_per\_class = 50 (ImageNet-10), 1000 (Split-MNIST)

Es werden 10 Wiederholungen pro Datensatz durchgeführt.

Die Ergebnisse der einzelnen Datensätze werden hier dargestellt. Für den Fall des verteilten Lernens auf zwei Geräten wird die Klassifikationsgenauigkeit der einzelnen Geräte nach dem Erlernen ihrer verfügbaren Klassen angegeben. Zusätzlich wird die finale Genauigkeit des „verschmolzenen“ Netzwerks gegeben. Als Referenz dienen die Ergebnisse des kontinuierlichen Lernens auf einem Gerät, da im besten Fall durch das verteilte Lernen keine schlechteren Ergebnisse erzielt werden sollen.

Zunächst findet die Auswertung für Split-MNIST statt. Dabei wurden auf Gerät 1 die Gruppen 0/1, 2/3 und 4/5 trainiert, während auf Gerät 2 die Gruppen 6/7 und 8/9 trainiert wurden. Die gemittelten Ergebnisse aus 10 Läufen sowie deren Standard-Abweichung sind in Tabelle 11 gegeben.

Tabelle 11: Klassifikationsgenauigkeit des verteiltem L DNN Algorithmus auf Split-MNIST

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithmus | Klassifikations-genauigkeit Gerät 1 in % | Klassifikations-genauigkeit Gerät 2 in % | Klassifikations-genauigkeit final in % |
| L DNN Algorithmus – 1 Gerät | - | - | 86,94 +/- 1,29 |
| L DNN Algorithmus – 2 Geräte | 88,44 +/- 0,82 | 95,02 +/- 0,44 | 86,56 +/- 0,91 |

Dieselbe Evaluation wird auf Basis des ImageNet-10 Datensatzes durchgeführt. Die Ergebnisse dieser Untersuchung sind in Tabelle 12 zu sehen. Die beiden Geräte haben dieselbe Anzahl an Klassen (fünf) gesehen. Die jeweiligen Klassen, die auf den Geräten trainiert werden, sind ebenso wie die Reihenfolge der Klassen zufällig ausgewählt.

Tabelle 12: Klassifikationsgenauigkeit des verteiltem L DNN Algorithmus auf ImageNet-10

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithmus | Klassifikations-genauigkeit Gerät 1 in % | Klassifikations-genauigkeit Gerät 2 in % | Klassifikations-genauigkeit final in % |
| L DNN Algorithmus – 1 Gerät | - | - | 76,4 +/- 1,2 |
| L DNN Algorithmus – 2 Geräte | 84,64 +/- 4,73 | 87,44 +/- 4,04 | 76,26 +/- 1,5 |

Die Ergebnisse für Split-MNIST und ImageNet-10 zeigen, dass mit separatem Training auf mehreren Geräten (hier zwei) dieselbe Genauigkeit erreicht werden kann wie mit dem Training auf einem einzelnen Gerät. Die Ergebnisse in Tabelle 11 und Tabelle 12 verdeutlichen diese Aussage. Zudem kann gesagt werden, dass durch das „Verschmelzen“ von Wissen eine schlechtere Genauigkeit auftritt. Die einzelnen Genauigkeiten von Gerät 1 und Gerät 2 auf ihren jeweiligen Testdaten sind besser als die finale Klassifikationsgenauigkeit. Dies hängt mit der komplexeren finalen Aufgabe zusammen, da dort statt 6 und 4 (für Split-MNIST) oder 5 und 5 Klassen (für ImageNet-10) nun 10 Klassen im Test-Datensatz vorkommen. Insgesamt kann auf Basis dieser Ergebnisse gesagt werden, dass das verteilte Lernen mit diesem Algorithmus funktioniert, da dort kein nennenswerter Performanz Verlust gegenüber dem zentralen Erlernen der Aufgabe auf einem Gerät auftritt. Somit eignet sich dieser Algorithmus zum Einsatz auf verteilten Systemen, die ihr Wissen ohne die jeweiligen Rohdaten austauschen müssen.

## Einfluss von Konsolidierungsschritten

Wie in der Konzeption beschrieben, gibt es die Möglichkeit das erlernte Wissen des inkrementellen Klassifikators zu konsolidieren. In diesem Prototyp wird die Konsolidierung durch eine Mittelwertbildung aller Repräsentationen einer einzelnen Klasse realisiert (für Details siehe Konzeption und Prototypenbeschreibung). Dadurch ist der Speicherbedarf um einiges geringer als ohne Konsolidierung. In diesem Testfall wird nun der genaue Einfluss der Konsolidierung auf die Klassifikationsgenauigkeit und den Speicherbedarf des inkrementellen Klassifikator in Modul B untersucht.

Es wird dieselbe Prozedur wie für die finalen Untersuchungen des kontinuierlichen Lernens genutzt (siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**). Es wird zusätzlich eine Konsolidierung der Repräsentationen durchgeführt. Es werden zwei Testfälle durchgeführt. Beim ersten Testfall wird nach dem Training jeder Gruppe eine Konsolidierung durchgeführt. Dieser Testfall wird im weiteren Verlauf in Graphiken und Tabellen „*Konsolidierung jeder Schritt*“ genannt. Im zweiten Testfall findet keine Konsolidierung während des Trainings der einzelnen Gruppen statt. Die Konsolidierung findet nach dem Training aller Gruppen/Klassen und vor der Bestimmung der Test-Genauigkeit statt. Dieser Fall wird im weiteren Verlauf „*Konsolidierung finaler Schritt*“ genannt. Als Referenz dienen die in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** erzielten Ergebnisse ohne Konsolidierung. Für die beiden Testfälle werden jeweils 10 Wiederholungen durchgeführt. Die im Folgenden genannten Ergebnisse beziehen sich dabei jeweils auf die Mittelwerte der erhaltenen Ergebnisse. Die Tests werden für Split-MNIST und ImageNet-10 durchgeführt.

Zunächst wird die Klassifikationsgenauigkeit der unterschiedlichen Testfälle auf Basis von Split-MNIST dargestellt. Die Ergebnisse für die beiden Testfälle sowie der Referenz (Keine Konsolidierung) sind in Abbildung 33 zu sehen. Die unterschiedlichen Kurven stellen dabei die Genauigkeiten für die jeweiligen Methoden der Konsolidierung über die Anzahl an erlernten Klassen dar.

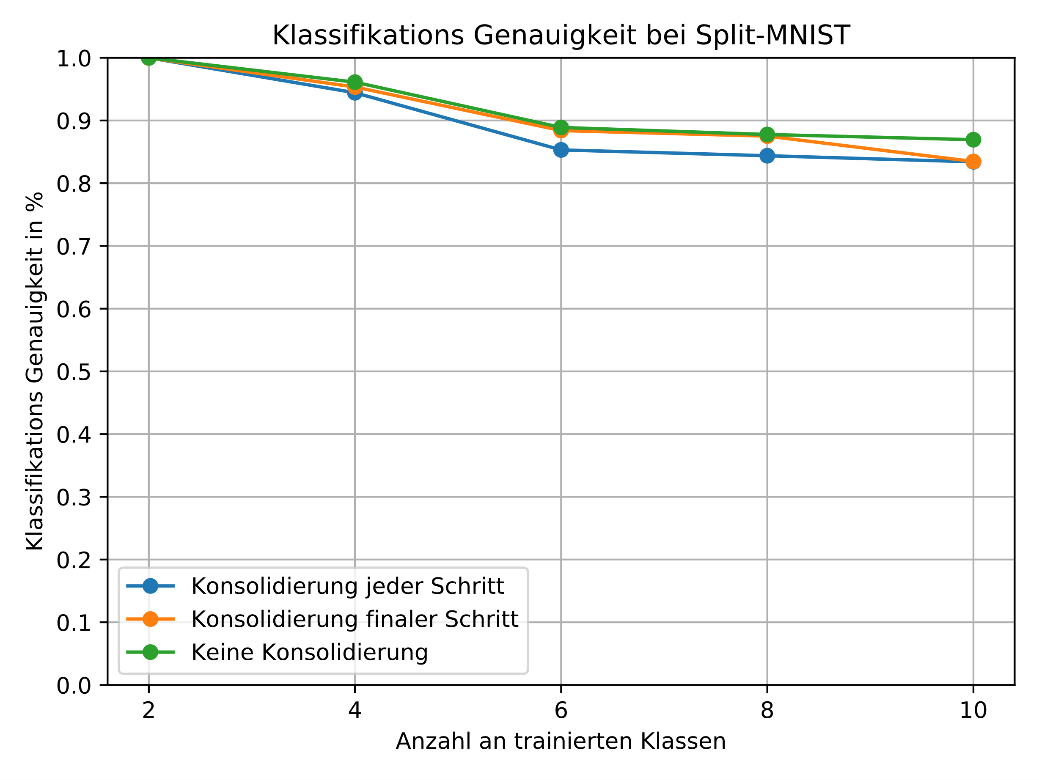


Abbildung 33: Klassifikationsgenauigkeit für unterschiedliche Konsolidierungsmethoden

Die gleiche Darstellung der Ergebnisse für ImageNet-10 ist in Abbildung 34 zu sehen.

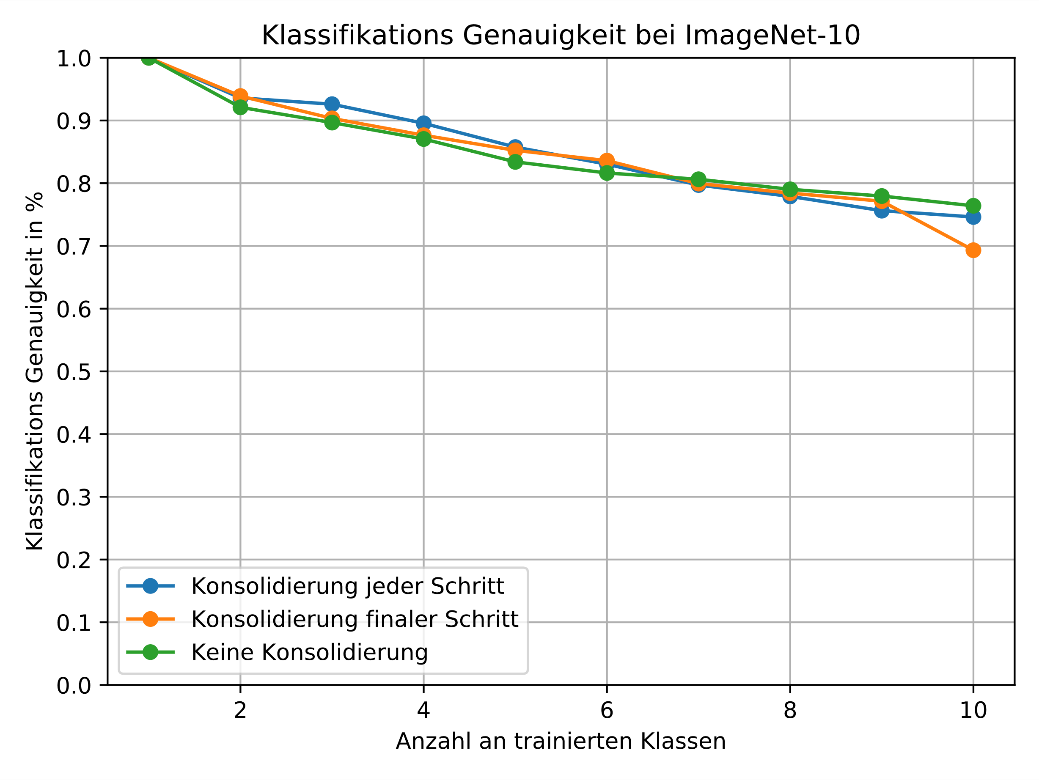


Abbildung 34: Klassifikationsgenauigkeit für unterschiedliche Konsolidierungsmethoden

Für eine sinnvolle Einschätzung und Bewertung wird der finale Speicherbedarf der unterschiedlichen Methoden angeschaut. Dieser wird inklusive der finalen Klassifikationsgenauigkeiten für Split-MNIST in Tabelle 13 zusammengefasst.

Tabelle 13: Vergleich von Speicherbedarf und finaler Klassifikationsgenauigkeit für unterschiedliche Methoden der Konsolidierung Split-MNIST

|  |  |  |
| --- | --- | --- |
| Konsolidierungs-methode | Finale Klassifikations-genauigkeit Split-MNIST in % | Finaler Speicherbedarf Split-MNIST in MB |
| Keine Konsolidierung | 86,94 +/-1,29 | 1,83 |
| Jeder Schritt | 83,41 +/- 1,64 | 0,1 |
| Finaler Schritt | 83,47 +/- 1,8 | 0,1 |

Tabelle 14 zeigt diesen Zusammenhang für ImageNet-10.

Tabelle 14: Vergleich von Speicherbedarf und finaler Klassifikationsgenauigkeit für unterschiedliche Methoden der Konsolidierung ImageNet-10

|  |  |  |
| --- | --- | --- |
| Konsolidierungs-methode | Finale Klassifikations-genauigkeit ImageNet-10 **i**n % | Finaler Speicherbedarf ImageNet-10 in MB |
| Keine Konsolidierung | 76,4 +/- 1,2 | 0,96 |
| Jeder Schritt | 74,62 +/- 2,19 | 0,1 |
| Finaler Schritt | 69,32 +/- 4,81 | 0,1 |

Anhand der erzielten Ergebnisse kann gesagt werden, dass bei Anwendungen mit sehr begrenztem Speicher die Konsolidierung eine gute Maßnahme sein kann, um den Speicherbedarf drastisch zu reduzieren und dabei geringe Genauigkeitseinbußen zu haben. Für Split-MNIST wird eine finale Klassifikationsgenauigkeit von ca. 83% mit beiden Konsolidierungsmethoden erreicht, was ca. 3 Prozentpunkte schlechter ist als ohne Konsolidierung. Jedoch ist der Speicherbedarf mit 0,1 MB auch nur 1/18 im Vergleich zu keiner Konsolidierung (siehe Tabelle 13). In Abbildung 33 kann gezeigt werden, dass bei einer Konsolidierung im finalen Schritt die Genauigkeit bis zum letzten finalen Testlauf identisch bleibt, da dort noch keine Konsolidierung stattgefunden hat und somit das Training und Testen bis dorthin identisch ist. Für Split-MNIST kann kein direkter Unterschied zwischen den beiden Konsolidierungsmethoden („*Jeder Schritt*“ und „*Finaler Schritt*“) gesehen werden, da beide nahezu identische Ergebnisse liefern.

Diese Aussage gilt nicht für ImageNet-10. Auch hier ist der Speicherbedarf mit 0,1 MB im Vergleich zu 0,96 MB um einiges geringer. Bei der Klassifikationsgenauigkeit gibt es jedoch auffällige Unterschiede. Mit der Konsolidierung nach jedem Schritt kann mit 74,62% Genauigkeit ein ähnliches Resultat wie ohne Konsolidierung (76,4%) erreicht werden. Bei der Konsolidierung nach dem finalen Schritt wird jedoch eine Genauigkeit von lediglich 69,32% mit deutlich erhöhter Varianz (4,81) erzielt (siehe Tabelle 14). Dies verdeutlicht den Einfluss der Konsolidierungsmethode für ein FuzzyARTMAP-Netzwerk, da das Training eines solchen Netzwerks stark von bereits bekannten Repräsentationen abhängt.

Der Grund für die schlechtere Performanz der Methode „finaler Schritt“ könnte darin liegen, dass während der Trainingsschritte viele Repräsentationen anderer Klassen vorliegen. Dies führt in der Regel zu einer erhöhten Anzahl an Repräsentationen für neue Klassen, um einen eindeutigen Sieger für diese Kategorie stellen zu können. Für einen Datensatz mit komplexen Klassen und Bilder wie ImageNet wird dann bei einer Konsolidierung im finalen Schritt separates Wissen über eine Klasse/Kategorie mit einer simplen Mittelwert-Logik verbunden. Dadurch werden unterschiedliche Repräsentationen „in ihrer Mitte“ zusammengefasst. Wenn die Methode „*Jeder Schritt*“ angewendet wird, ist während des Trainings einer neuen Klasse nur eine Repräsentation pro alte Klasse vorhanden. Dadurch bildet das FuzzyARTMAP-Netzwerk weniger Repräsentationen mithilfe der optimierten Lernrate . Diese generalisierten Repräsentationen scheinen robuster zu sein als die mithilfe des Mittelwertes konsolidierten Repräsentationen.

Alles in allem kann mithilfe der Konsolidierung der Speicherbedarf drastisch reduziert. In Abhängigkeit der gewählten Konsolidierungsmethode wird dabei die Klassifikationsgenauigkeit nur leicht verringert. Mit der Methode „*Jeder Schritt*“ können ähnliche Ergebnisse wie ohne Konsolidierung erreicht werden mit 1/18 (Split-MNIST) und 1/9 (ImageNet-10) des ursprünglichen Speicherbedarfs. Dies zeigt, dass Konsolidierung für eine spätere Anwendung in einem speicherarmen Endgerät interessant sein kann.

Als Ausblick könnte für die Konsolidierung eine mathematisch komplexere Formel anstatt dem simplen Mittelwert genutzt werden. Zum Beispiel könnten nur Repräsentationen einer Klasse konsolidiert werden, die eine Ähnlichkeit (z.B. *cosine-*Similarity) über einem definierten Schwellwert haben. Dadurch kann das konsolidieren von im Feature-Raum unterschiedlichen Repräsentationen einer Klasse vermieden werden. Als Folge würden die Klassen nicht durch eine, sondern durch mehrere ausgewählten Repräsentationen dargestellt, die wiederum eine Vielzahl an ähnlichen Repräsentationen bündeln und darstellen. Dies kann im Rahmen dieser Arbeit jedoch aufgrund von Zeitgründen nicht weiterverfolgt werden.

Als weiteren Ausblick kann mit der hier vorhandenen Logik ein intelligenter Zeitpunkt für die Konsolidierung gewählt werden. Es muss nicht nach dem Training einer neuen Klasse stattfinden, wenn dafür keine Notwendigkeit herrscht, sondern könnte in realen Anwendungsfällen zum Beispiel zu dem Zeitpunkt erfolgen, an dem 90% des verfügbaren Speichers belegt ist. Wie in den hier beschriebenen Testfällen gezeigt, kann bei geringem Genauigkeitsverlust (2-3 Prozentpunkte) eine Menge Speicher freigegeben werden (Reduktion auf 1/18 und 1/9 des ursprünglichen Bedarfs).

## Gesamter ImageNet-Datensatz

Für eine finale Untersuchung des Algorithmus auf einem komplexen Datensatz mit vielen Klassen wird der ImageNet-2012 Datensatz genutzt. Dieser beinhaltet 1000 Klassen mit über 1 Millionen Trainingsbildern und 50.000 Testbilder. Die Ergebnisse auf diesem Datensatz dienen als Vergleich zu anderen inkrementellen Klassifikatoren. Der Datensatz ist detaillierter in der Evaluierungsspezifikation und in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** dieses Dokuments definiert. Es wird zunächst das inkrementelle Klassenlernen auf einem Gerät untersucht, und später eine Untersuchung des Lernverhaltens auf zwei verteilten Geräten durchgeführt.

Die in Kapitel 4 der Evaluierungsspezifikation genannten Testfälle für ImageNet werden nun durchgeführt. Für eine Vergleichbarkeit mit anderen Algorithmen wird das Netzwerk nicht wie in der Evaluierungsspezifikation beschrieben zunächst auf 900 zufälligen Klassen vortrainiert, sondern er wird inkrementell mit allen 1000 Klassen trainiert. Für den Fall des verteilten Lernens auf zwei Geräten werden jeweils 500 Klassen pro Gerät trainiert.

Es werden die in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** und **Fehler! Verweisquelle konnte nicht gefunden werden.** genannten Parameterwerte für ImageNet-10 auch für den gesamten ImageNet Datensatz genutzt. Variiert wird die Anzahl an inkrementellen Schritten (Trainings-Gruppen). Dies verändert die Anzahl an Klassen, die pro Trainingsschritt erlernt werden. Es werden dabei folgende Werte für die Anzahl an Klassen pro Trainingsschritt gewählt: [1, 50, 100, 1000]. Pro Fall wird aufgrund der großen Datenmenge anstatt wie bisher 10 lediglich 1 Wiederholung durchgeführt. Zudem werden aufgrund der großen Anzahl an Klassen lediglich 10 Trainingsbilder pro Klasse genutzt anstatt 100 wie für ImageNet-10. Als Referenz werden die in [49] aufgeführten Ergebnisse für ImageNet genutzt.

Zunächst wurde der Algorithmus mit 1 inkrementellem Schritt trainiert. Das heißt, dass kein inkrementelles Lernen stattfindet, sondern alle 1000 Klassen im ersten Trainingsschritt erlernt werden. Es konnte eine finale Klassifikationsgenauigkeit auf den Testdaten von 39,1% erreicht werden bei einem Speicherbedarf von 85,2 MB für Modul B. Da hier kein inkrementelles Lernen stattfindet, wird auf eine graphische Darstellung dieses einen Wertes verzichtet.

Mit 10 inkrementellen Schritten wird am Ende auf allen Testdaten eine Klassifikationsgenauigkeit von 39,3% bei einem Speicherbedarf von 87,2 MB erreicht. Da diese Anzahl an inkrementellen Schritten auch in [49] für die finale Auswertung genutzt wird, werden die erreichten Ergebnisse in Relation zu dem bereits in der Konzeption beschriebenen *iCaRL*-Algorithmus sowie dem *Learning without Forgetting* (LwF) [50] gesetzt. Die Ergebnisse sind in Abbildung 35 dargestellt.

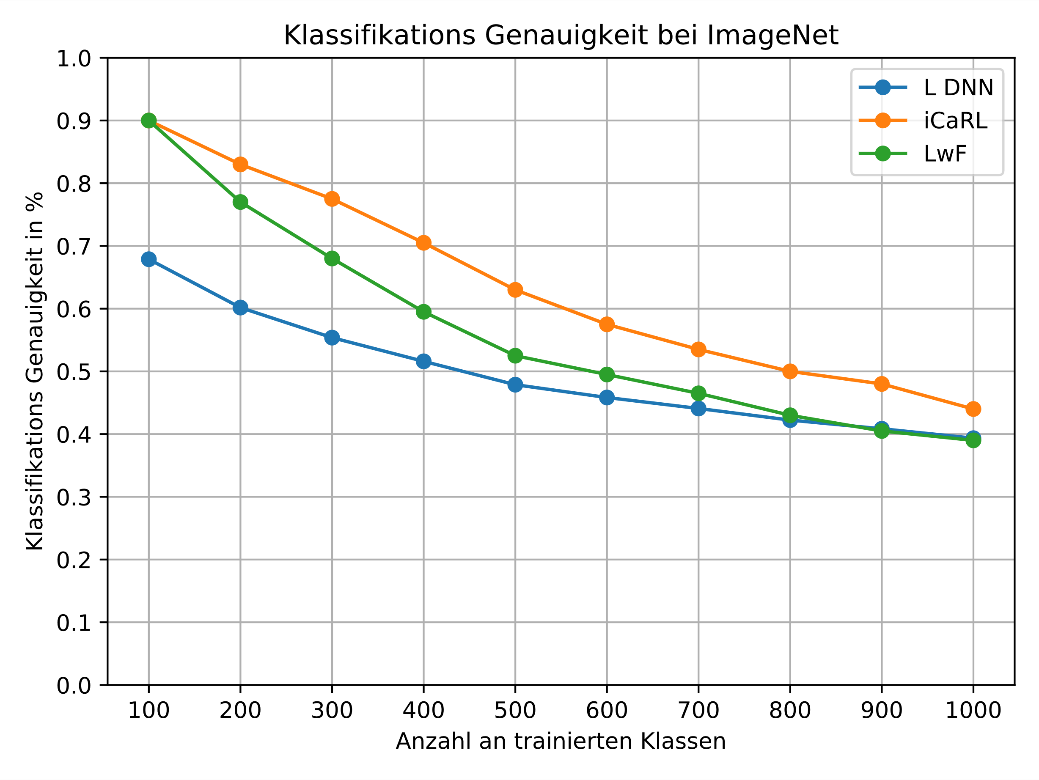


Abbildung 35: Klassifikationsgenauigkeit bei ImageNet für unterschiedliche inkrementelle Lernalgorithmen

Zusätzlich wird in Abbildung 36 zu den bereits beschriebenen Kurven die Klassifikationsgenauigkeit des L DNN Algorithmus mit 20 inkrementellen Schritten dargestellt (rote Kurve). Die anderen Kurven sind identisch zu Abbildung 35 und nur als Referenz eingezeichnet.

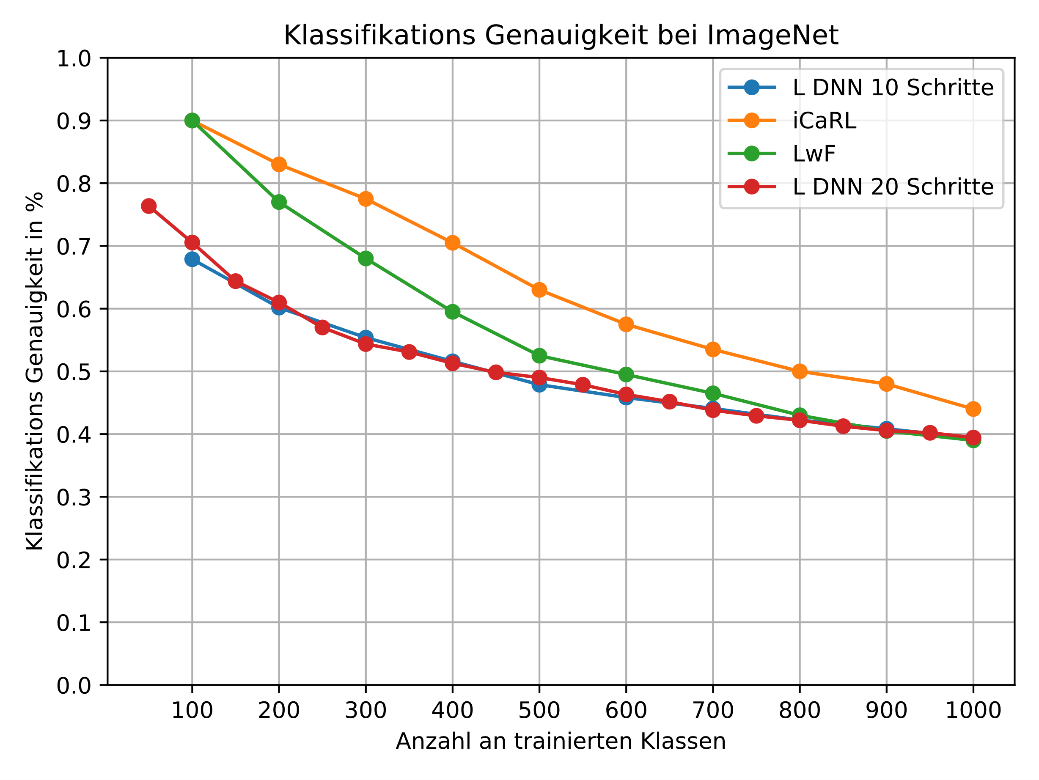


Abbildung 36: Klassifikationsgenauigkeit bei ImageNet mit unterschiedlicher Anzahl an inkrementellen Schritten

Beide Algorithmen, iCaRL und LwF, nutzen ein 18-Layer ResNet zur Feature-Extrahierung. Der iCaRL-Algorithmus speichert 20.000 Exemplare in dem referenzierten Versuch ab. LwF arbeitet ohne Speicherung von Exemplaren und trainiert neue unabhängige Fully Connected Layer für jeden inkrementellen Schritt. Jeder inkrementelle Lernschritt hat bei diesen beiden Algorithmen 100 Epochen, während der L DNN Algorithmus lediglich eine Epoche pro inkrementellen Schritt durchführt. In Tabelle 15 sind die finalen Genauigkeiten und der Speicherbedarf der genannten Algorithmen zusammengefasst.

Tabelle 15: Finale Klassifikationsgenauigkeiten ImageNet

|  |  |  |
| --- | --- | --- |
| Algorithmus | Finale Klassifikations-genauigkeit ImageNet **i**n % | Finaler Speicherbedarf ImageNet-10 in MB |
| L DNN  (ein inkrementeller Schritt) | 39,1 | 527,2 |
| L DNN  (10 inkrementelle Schritte) | 39,3 | 530,5 |
| L DNN  (50 inkrementelle Schritte) | 39,4 | 528,8 |
| iCaRL | 44 | 2123 |
| LwF | 39 | - |

Für L DNN ist der gesamte Speicherbedarf für Modul A und Modul B angegeben. Für iCaRL und LwF konnten keine konkreten Angaben zum Speicherbedarf gefunden werden. Für iCaRL wurde der Speicherbedarf mithilfe der durchschnittlichen Größe eines Bildes (ca. 106 KB) des ImageNet-Datensatz ermittelt für 20.000 gespeicherte Exemplare. Zusätzlich würde noch der Speicherbedarf des Feature-Extrahierers dazu kommen. Für LwF konnte keine Angabe für den Speicherbedarf gefunden werden und auch keine sinnvolle Abschätzung getroffen werden.

Auf Basis der Ergebnisse, die in Tabelle 15 und in Abbildung 35 dargestellt sind, wird der L DNN Algorithmus final bewertet. Dafür wird zunächst der L DNN Algorithmus mit 10 inkrementellen Schritten mit iCaRL und LwF verglichen. In Abbildung 35 ist zu sehen, dass der L DNN Algorithmus vom ersten inkrementellen Schritt (100 Klassen) an eine deutlich geringe Klassifikationsgenauigkeit hat (67,9%) als iCaRL und LwF (beide 90%). Dies kann mit dem gewählten Feature-Extrahierer begründet werden. Mit MobileNet-v2 wurde für den L DNN Algorithmus ein Kompromiss zwischen Speicherbedarf und Genauigkeit getroffen. LwF und iCaRL nutzen jeweils eine ResNet-Architektur für die Feature-Extraktion. Diese Architektur erzielt auf ImageNet bessere Genauigkeiten als MobileNet-v2 (siehe Konzeption), wodurch eine höhere Klassifikationsgenauigkeit mit den hier genutzten Algorithmen möglich ist. Ebenfalls ist in Abbildung 35 der Verlauf über die Anzahl an trainierten Klassen zu sehen. Der L DNN Algorithmus ist hier wesentlich stabiler als die anderen beiden Algorithmen, welche mit zunehmender Anzahl an trainierten Klassen deutliche stärker an Genauigkeit verlieren.

Tabelle 16 stellt den relativen verbleibenden Anteil der Klassifikationsgenauigkeit für die einzelnen Algorithmen dar. Dafür wird die Genauigkeit nach dem letzten finalen Schritt (1000 Klassen) durch die Genauigkeit nach dem ersten Schritt (100 Klassen) dividiert, um das relative Verhältnis zu erhalten.

Tabelle 16: Relativer Erhalt der Klassifikationsgenauigkeit auf ImageNet

|  |  |
| --- | --- |
| Algorithmus | Relativer Erhalt Klassifikationsgenauigkeit in % |
| L DNN  (10 inkrementelle Schritte) | 57,9 |
| iCaRL | 48,9 |
| LwF | 43,3 |

Der L DNN Algorithmus erreicht nach dem finalen Training auf 1000 Klassen noch ca. 58% seiner anfänglichen Genauigkeit, während iCaRL und LwF mit ca. 49% (iCaRL) und ca. 43% (LwF) jeweils weniger als die Hälfte erreichen.

Auf Basis dieser Ergebnisse kann gesagt werden, dass der L DNN Algorithmus für eine große Anzahl an Klassen stabiler ist und im Vergleich zu den anderen Algorithmen auf großen Daten „besser skaliert“.

Die finale Genauigkeit des L DNN Algorithmus ist dabei identisch wie die des LwF-Algorithmus, der jedoch eine komplexere Trainingsstrategie verfolgt (Training einzelner Fully-Connected Layer mithilfe des Backpropagation-Algorithmus auf Basis der neuen Samples). Hier ist kein Vergleich beim Speicherbedarf möglich, da für LwF keine Werte vorliegen und der Speicherbedarf nicht abgeschätzt werden kann. Der iCaRL-Algorithmus erreicht eine bessere finale Klassifikationsgenauigkeit mit 44% gegenüber dem L DNN Algorithmus (ca. 39%), jedoch ist der Speicherbedarf hier um einiges höher. Für die Speicherung der Exemplare benötigt iCaRL bei diesem Test über 2 GB, während der gesamte L DNN Algorithmus lediglich ca. 530 MB benötigt. Unter Berücksichtigung der genutzten Feature-Extrahierer ist es möglich, dass der L DNN Algorithmus mit einem leistungsfähigeren Extrahierer eine bessere Genauigkeit als iCaRL erreichen kann. Der Speicherbedarf des L DNN würde steigen, jedoch vermutlich weiterhin geringer sein als der des iCaRL. Der gesteigerte Speicherbedarf könnte in einzelnen Anwendungsfällen für eine bessere Genauigkeit akzeptiert werden.

Im Weiteren wird der Einfluss von einer unterschiedlichen Anzahl an inkrementellen Schritten für den L DNN Algorithmus bei einem großen Datensatz untersucht. Hierzu wurden 20 statt 10 inkrementelle Schritte durchgeführt. Damit werden bei einem inkrementellen Trainingsschritt 50 zufällige Klassen trainiert. Auf Basis der in [49] angegebenen Resultate führt eine erhöhte Anzahl an inkrementellen Schritten bei LwF und iCaRL zu einer schlechteren finalen Klassifikationsgenauigkeit. Speziell LwF ist deutlich sensitiver zu der Anzahl an inkrementellen Trainingsschritten. Dieses Verhalten ist für den L DNN Algorithmus nicht zu beobachten. In Abbildung 36 kann kein nennenswerter Unterschied zwischen den Kurven mit 10 und 20 inkrementellen Schritten gesehen werden. Auch die finale Klassifikationsgenauigkeit ist (nahezu) identisch. Dieses Verhalten ist für spätere reale Anwendungen von großer Bedeutung. In relevanten Anwendungen des kontinuierlichen Lernens können viele inkrementelle Schritte auftreten, da einzelne Klassen nach und nach während dem Betrieb auftreten. Dort soll eine gute Klassifikationsgenauigkeit ermöglicht werden. In diesem Fall ist für LwF und iCarL eine deutlich geringere Performanz im Vergleich zu den bekannten Ergebnissen auf den hier genutzten Test-Datensätzen zu erwarten. Für den L DNN Algorithmus kann erwartet werden, dass die hier gezeigte und erreichte Performanz auch bei vielen inkrementellen Schritten erreicht werden kann.

Dieses hier beobachtete Verhalten des L DNN Algorithmus ist positiv für die Nutzung des L DNN Algorithmus in weiteren (realen) Anwendungen. Der Algorithmus erfüllt die grundlegenden Eigenschaften eines kontinuierlich lernenden Algorithmus, und kann auf Basis weniger Trainingsdaten robust neue Klassen erlernen. Zudem verhält er sich gegenüber einer großen Anzahl an Klassen stabil und ist ebenfalls nicht sensitiv gegenüber der Anzahl an inkrementellen Trainingsschritten.

Es sollte weiterhin untersucht werden, inwieweit die Klassifikationsgenauigkeit des Algorithmus durch einen besseren Feature-Extrahierer in Modul A verbessert werden kann. Wenn hier eine weitere Verbesserung der Genauigkeit erreicht werden kann, hat der Algorithmus das Potenzial auch in realen Anwendungen sehr gute Resultate zu erzielen. Zudem wäre eine Untersuchung auf ImageNet mit 1000 inkrementellen Schritten (1 Klasse pro Schritt) interessant für die im vorigen Abschnitt getroffene Aussage. Weiterhin sollte das Verhalten des verteilten Lernens für 2 (oder mehrere) Endgeräte auf ImageNet untersucht werden.

# Demonstrator

# Zusammenfassung und Ausblick

# Literatur

|  |  |
| --- | --- |
| [1] | M. Luciw, S. Olivera, A. Gorshechnikov, J. Wurbs, H. M. Ames und M. Versace, „Systems and Methods to enable Continual, Memory-Bounded learning in Artificial Intelligence and Deep Learning Continuously operating Applications across networked Compute Edges“. United States of America Patent US 2018/0330238 A1, 15 November 2018. |
| [2] | Neurala Inc., „Lifelong Deep Neural Networks - Tech Summary,“ [Online]. Available: https://info.neurala.com/hubfs/docs/ Neurala\_LifelongDNNWhitepaper.pdf. [Zugriff am 7 Mai 2019]. |
| [3] | Neurala Inc., „Neurala vs. Open Soruce,“ [Online]. Available: https://info.neurala.com/hubfs/docs/Open%20source%20vs.%20Neurala.pdf. [Zugriff am 7 Mai 2019]. |
| [4] | I. Goodfellow, Y. Bengio und A. Courville, Deep Learning, MIT Press, 2016. |
| [5] | C. M. Bishop, Pattern Recognition and Machine Learning, Springer, 2006. |
| [6] | M. A. Nielsen, Neural Networks and Deep Learning, Determination Press, 2015. |
| [7] | A. Zang, Z. C. Lipton, M. Li und A. J. Smola, Dive into Deep Learning, 2019. |
| [8] | G. E. Hinton, S. Osindero und Y.-W. Teh, „A fast learning algorithm for deep belief nets,“ *Neural Computation,* Bd. 18, Nr. 7, pp. 1527-1554, 2006. |
| [9] | B. Yang, *Lecture Notes Deep Learning,* Stuttgart, 2018. |
| [10] | D. Michie und D. J. Spiegelhalter, Machine Learning, Neural and Statistical Classification, Leeds: C. C. Taylor, 1994. |
| [11] | Y. LeCun, L. Bottou, Y. Bengio und P. Haffner, „Gradient-based Learning applied to document recognition,“ *Proceedings of the IEEE,* pp. 2279-2324, November 1998. |
| [12] | R. M. French, „Catastrophic forgetting in connectionists networks,“ *Trends in Cognitive Sciences,* pp. 128-135, April 1999. |
| [13] | Y.-c. Hsu, Y.-c. Liu und Z. Kira, „Re-evaluating Continual Learning Scenarios : A Categorization and Case for Strong Baselines,“ in *32nd Conference on Neural Information Processing Systems (NIPS2018)*, Montréal, 2018. |
| [14] | G. I. Parisi, R. Kemker, J. L. Part, C. Kanan und S. Wermter, „Continual lifelong learning with neural networks: A review,“ *Neural Networks,* pp. 54-71, 2019. |
| [15] | W. Abraham und A. Robins, „Memory retention - The synaptic stability versus plasticity dilemma,“ *Trends in neurosciences,* pp. 73-8, 03 2005. |
| [16] | C. Kortge, „Episodic Memory in Connectionist Networks,“ *Proceedings of the 12th Annual Conference of Cognitive Science Society,* pp. 764-771, 01 Januar 1993. |
| [17] | R. Kemker, M. McClure, A. Abitino, T. Hayes und C. Kanan, „Measuring Catastrophic Forgetting in Neural Networks,“ November 2017. |
| [18] | J. Kirkpatrick, R. Pascanu, N. Rabinowitz, J. Veness, G. Desjardins, A. A. Rusu, K. Milan, J. Quan, T. Ramalho, A. Grabska-Barwinska, D. Hassabis, C. Clopath, D. Kumaran und R. Hadsell, „Overcoming catastrophic forgetting in neural networks,“ *Proceedings of the National Academy of Sciences,* pp. 3521-3526, 2017. |
| [19] | C. Fernando, D. Banarse, C. Blundell, Y. Zwols, D. Ha, A. A. Rusu, A. Pritzel und D. Wierstra, „PathNet: Evolution Channels Gradient Descent in Super Neural Networks,“ 2017. |
| [20] | A. Seff, A. Beatson, D. Suo und H. Liu, „Continual Learning in Generative Adversarial Nets,“ 23 Mai 2017. |
| [21] | C. V. Nguyen, Y. Li, T. D. Bui und R. E. Turner, „Variational Continual Learning,“ 03 November 2017. |
| [22] | H. Shin, J. K. Lee, J. Kim und J. Kim, „Continual Learning with Deep Generative Replay,“ *Proceedings of 31st Conference on Neural Information Processing Systems (NIPS 2017),* 2017. |
| [23] | J. L. McClelland und B. L. McNaughton, „Why There Are Complementary Learning Systems in the Hippocampusand Neocortex: Insights From the Successes and Failures ofConnectionist Models of Learning and Memory,“ *Psychological Review,* pp. 419-457, 1995. |
| [24] | S. A. Rebuffi, A. Kolesnikov, G. Sperl und C. H. Lampert, „iCaRL: Incremental classifier and representation learning,“ *Proceedings - 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017,* pp. 5533-5542, Januar 2017. |
| [25] | G. A. Carpenter und S. Grossberg, „Adaptive Resonance Theory,“ in *The Handbook of Brain Theory and Neural Networks*, Boston, MIT Press, 2002. |
| [26] | A. A.-m. Merten, „Adaptive Resonance Theory [ART] - Ein neuer Ansatz lernender Computer -,“ Universität Ulm, Ulm. |
| [27] | V. Hedge und S. Usmani, „Parallel and Distributed Deep Learning,“ *Tch Report,* 2016. |
| [28] | T. Ben-Nun und T. Hoefler, „Demystifying Parallel and Distributed Deep Learning: An In-Depth Concurrency Analysis,“ 2018. |
| [29] | J. Konecny, B. H. McMahan, D. Ramage und P. Richtarik, „Federated Optimization: Distributed Machine Learning for On-Device Intelligence,“ pp. 1-38, 2016. |
| [30] | Q. Yang, Y. Liu, T. Chen und Y. Tong, „Federated Machine Learning: Concept and Applications,“ Bd. 10, Nr. 2, pp. 1-19, 2019. |
| [31] | D. Jia, D. Wei, R. Socher, L. Li-Jia, L. Kai und F.-F. Li, „ImageNet: A large-scale hierarchical image database,“ *2009 IEEE Conference on Computer Vision and Pattern Recognition,* pp. 248-255, 2009. |
| [32] | J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li und L. Fei-Fei, „ImageNet: A Large-Scale Hierarchical Image Database,“ *2009 IEEE Conference on Computer Vision and Pattern Recognition,* pp. 248-255, 2009. |
| [33] | M. A. E. Muhammed, A. A. Ahmed und T. A. Khalid, „Benchmark Analysis of Popular ImageNet Classification Deep CNN Architectures,“ *Proceedings of the 2017 International Conference On Smart Technology for Smart Nation, SmartTechCon 2017,* pp. 902-907, 2018. |
| [34] | A. Krizhevsky, I. Sutskever und H. G. E., „ImageNet Classification with Deep Convolutional Neural Networks,“ *Advances in Neural Information Processing Systems 25,* pp. 1097-1105, 2012. |
| [35] | K. Sinhal, „CV-Tricks,“ 2017. [Online]. Available: https://cv-tricks.com/cnn/understand-resnet-alexnet-vgg-inception/. [Zugriff am 5 Juni 2019]. |
| [36] | Google Brain Team, „TensorFlow Guide,“ Google Brain, [Online]. Available: https://www.tensorflow.org/guide/tensors. [Zugriff am 29 Mai 2019]. |
| [37] | K. Simonyan und A. Zisserman, „Very Deep Convolutional Networks For Large-Scale Image Recognition,“ in *International Conference on Learning Representations 2015*, San Diego, 2015. |
| [38] | K. He, X. Zhang, S. Ren und J. Sun, „Deep residual learning for image recognition,“ *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* pp. 770-778, Dezember 2015. |
| [39] | C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke und A. Rabinovich, „Going deeper with convolutions,“ *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* pp. 1-9, Juni 2015. |
| [40] | C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens und Z. Wojna, „Rethinking the Inception Architecture for Computer Vision,“ *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* pp. 2818-2826, Dezember 2016. |
| [41] | A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto und H. Adam, „MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications,“ *CoRR,* 2017. |
| [42] | M. Sandler, A. Howard, M. Zhu, A. Zhmoginov und L. C. Chen, „MobileNetV2: Inverted Residuals and Linear Bottlenecks,“ *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* pp. 4510-4520, 2018. |
| [43] | M. Sandler und A. G. Howard, „Google AI Blog,“ Google AI, 3 April 2018. [Online]. Available: https://ai.googleblog.com/2018/04/mobilenetv2-next-generation-of-on.html. [Zugriff am 5 Juni 2019]. |
| [44] | C. Lampert, „Institue of Science and Technology Austria,“ 25 August 2018. [Online]. Available: https://pub.ist.ac.at/~chl/talks/lampert-vsssw2018.pdf. [Zugriff am 07 Juni 2019]. |
| [45] | T. Kasuba, „Simplified Fuzzy Artmap,“ *AI Expert,* pp. 18-25, 1993. |
| [46] | Generation Robots, „Generation Robots,“ [Online]. Available: https://www.generationrobots.com/media/raspi3-datasheet.pdf. [Zugriff am 06 Juni 2019]. |
| [47] | O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein, A. C. Berg und L. Fei-Fei, „ImageNet Large Scale Visual Recognition Challenge,“ 30 Januar 2015. |
| [48] | G. M. van de Ven und A. S. Tolias, „Three continual learning scenarios and a case for generative replay,“ in *International Conference on Learning Representations*, New Orleans, 2019. |
| [49] | Y. Wu, C. Yinpeng, L. Wang, Y. Ye, Z. Liu, G. Yandong und Y. Fu, „Large Scale Incremental Learning,“ *CoRR,* Mai 2019. |
| [50] | Z. Li und D. Hoiem, „Learning without Forgetting,“ *IEEE Transactions on Pattern Analysis and Machine Intelligence,* pp. 2935-2947, 2018. |

# Erklärung

Ich erkläre, die Arbeit selbständig verfasst und bei der Erstellung dieser Arbeit die einschlägigen Bestimmungen, insbesondere zum Urheberrechtsschutz fremder Beiträge, eingehalten zu haben. Soweit meine Arbeit fremde Beiträge (z. B. Bilder, Zeichnungen, Textpassagen) enthält, erkläre ich, dass diese Beiträge als solche gekennzeichnet sind (z. B. Zitat, Quellenangabe) und ich eventuell erforderlich gewordene Zustimmungen der Urheber zur Nutzung dieser Beiträge in meiner Arbeit eingeholt habe.

Unterschrift:

Stuttgart, den <TT.MM.JJJJ>