DHBW
Duale Hochschule
Baden-Württemberg
Ravensburg
Campus Friedrichshafen

# Dokumentation

## Training eines neuronalen Netzes

## Abgabe digitale Bildverarbeitung

Studiengang Elektrotechnik

Studienrichtung Fahrzeugelektronik

Duale Hochschule Baden-Württemberg Ravensburg, Campus Friedrichshafen

von

Martin Förstemann

| | |
|---|---|
| Abgabedatum: | 16. Dezember 2023 |
| Bearbeitungszeitraum: | 12.11.2023 - 05.01.2024 |
| Matrikelnummer: | 8488669 |
| Kurs: | TFE21-2 |

# 1 Konzept und Rahmenbedingungen

Zu Beginn werden zu erreichende Trainingsziele für das Netz und die Datenvorverarbeitung gesetzt. Um unabhängig anderer Rechenleistungen zu sein und damit auch dem Anspruch der Nachhaltigkeit gerecht zu werden soll das gesamte Netz auf der lokalen Hardware gerechnet werden. Die gesetzten Benchmarks sind dabei:

1. Alle Berechnungen und Trainings sollen auf der lokalen Hardware erfolgen.
2. Die Trainings- und Testdaten sollen in unter 30 s verarbeitet werden
3. Der Datensatz soll nicht maßgeblich vergrößert werden[1]
4. Das Modell selbst soll in unter einer Minute trainiert werden können
5. Die Anzahl der Parameter soll unter 1000 betragen
6. Die Genauigkeit auf den Testdatensatz soll bei über 90% liegen.

Das methodische Vorgehen, die in der Liste 1 aufgezeigten Vorgaben zu erreichen sieht wie folgt aus:

Es wird ein ursprüngliche Netz aufgestellt, das mit dem unbearbeiteten MNIST-Datensatz eine sehr hohe Accuracy aufweist. Dieses Grund-Netz wird Schritt für Schritt immer weiter an die Parametervorgaben angenähert. Im Quellcode ist lediglich das Grundnetz und das resultierende Netz dokumentiert, die Zwischenschritte sind nicht erläutert.

# 2 MNIST-Daten Vorbereitung

Um dem Netz das Lernen der Daten zu erleichtern und klarere Strukturen zu erkennen, werden alle Graustufen aus dem Datensatz eliminiert. Mit einer definierten Schwelle wird für jedes Pixel entschieden, ob es schwarz oder weiß ist. Diese Binarisierungstechnik trägt dazu bei, das Rauschen zu minimieren und die Daten zu vereinfachen.

[1] Z.B. durch Spiegeln der Bilder und somit Verdopplung der Bilderanzahl

Folglich existieren nur noch 0 und 1 Werte die deutlich einfacher interpretiert werden können. Zudem reduziert es die Datenmenge deutlich und hilft bei einer schnelleren Datenverarbeitung. Hier wurde die Datenmenge genau halbiert (siehe Code: vorher $37632 \cdot 10^4$ Bytes, nachher $18816 \cdot 10^4$ Bytes). Zusätzlich kann die klare Unterscheidung zwischen schwarz und weiß bei der Kantendetektierung helfen. Diese bilden den zweiten Bearbeitungsschritt.

Nach der Binärisierung wird ein Sobel-Filter angewendet, der die Bilder nach Kanten untersucht. Er besteht aus zwei Kernels, die jeweils horizontal und vertikal nach Kanten suchen. Das macht insofern Sinn, da unser metrisches Zahlensystem viele dieser Kanten besitzt. Vereinfacht wird diese Suche durch die vorherige Binärisierung.

Anschließend werden die Daten mit einem Gauß-Filter bearbeitet, um die Kanten zu glätten und etwaige Treppenartefakte (die durch die Binärisierung entstehen können) an den Kanten zu minimieren.

Als letze Vorverarbeitung wird eine One-Hot-Codierung mit den Labeln durchgeführt. Es wandelt die Labels in einen Vektor um, der nur Nullen enthält, außer für die repräsentative Klasse. Das ist insofern passend, da es sich um eine Klassifizierungsaufgabe handelt. Die Funktion `to_categorical` aus der `tensorflow.keras.utils`-Bibliothek wird verwendet, um Klassenlabels in eine sogenannte One-Hot-Kodierung umzuwandeln.

Die Anzahl der Trainingsdaten wurden vorerst nicht reduziert, da es für das Einhalten der oben genannten Vorgaben nicht nötig ist.

# 3 Training des Netzes

Zu Beginn wird ein Netz aufgestellt, das vornehmlich eine hohe Genauigkeit aufweist, ohne die Menge an Parametern, Trainingszeit o.ä. zu beachten.

Die Anzahl der Parameter, Labels oder die Berechnungszeiten sollen folglich in der zweiten Version des Netzes optimiert werden.

Das optimierte Netz startet mit dem Layer

**Listing 1:** Optimierter erster Layer des Netzes

```
1 tf.keras.layers.Conv2D(16, (3, 3), activation=tf.keras.
  layers.LeakyReLU(alpha=0.03), input_shape=(28, 28, 1))
```

und hat nur noch 16 Merkmalerkennungen. Die Leaky ReLU-Funktion wird verwendet, um früh vermeintlich falsch abgestrafte Merkmale nicht 'sterben' zu lassen. Das wird in der zweiten Schicht ebenso verwendet, aber bereits mit einem reduzierten Faktor, da die relevanten Merkmale hier schon deutlich mehr ausgeprägt sein sollten. Ab dem dritten Convolutional-Layer wird die normale ReLU als Aktivierungsfunktion genutzt.

Um die Gesamtanzahl der Parameter zu verringern, wird die Filteranzahl der Convolutional-Layer reduziert. Zudem wird die Kernel-Dimension angepasst, um genauere Ergebnisse zu erzielen. Es wird ein Feature Detector von (6, 1) verwendet, um horizontale Strukturen zu erkennen, und im späteren Layer ein (1, 6) Feature Detector, um vertikale Merkmale zu erkennen. Das deckt sich mit der Idee, die Kanten zu finden, die im Voraus im Datensatz durch den Sobel-Filter markiert wurden. Die Dimension des Feature Detectos ist hier auffällig, da sie nicht dem gewöhnlichen Ansatz folgt eine Zweierptenz zu verwenden. Für die hier verwendete Architektur hat es aber bei geringer Parameteranzahl sehr gut funktioniert. Die `MaxPooling2D`-Layer werden verwendet um die räumliche Dimension zu reduzieren und damit die Berechnungskosten zu senken. Die `Flatten`-Schicht bereitet die Daten für den `Dense`-Layer vor. Die Dense-Schicht mit 16 Neuronen hat die Aufgabe, abstrakte Merkmale aus den vorherigen Schichten zu gewinnen. Durch die Anwendung der ReLU-Aktivierungsfunktion werden nicht-lineare Aspekte betont, wobei negative Werte unterdrückt werden. Ziel ist es hier, eine repräsentative Daten-Darstellung zu erzeugen, während die Parameteranzahl moderat gehalten wird. Die Dropout-Schicht wird hinzugefügt, um Overfitting zu verhindern. Sie deaktiviert zufällig 2,5% der Neuronen während des Trainings, was dazu beiträgt, dass das Modell nicht zu sehr auf spezifische Muster der Trainingsdaten

angewiesen ist. Dies verbessert die Generalisierungsfähigkeit des Modells. Die letzte Dense-Schicht mit 10 Neuronen entspricht den 10 Klassen des MNIST-Datensatzes (0 bis 9). Durch die Anwendung der Softmax-Aktivierungsfunktion wird die Ausgabe in Wahrscheinlichkeiten für jede Klasse umgewandelt. Das Neuron mit der höchsten Wahrscheinlichkeit wird dann als die vom Modell vorhergesagte Klasse interpretiert. Diese entscheidende Schicht führt die endgültige Klassifikation durch und bildet den Output des neuronalen Netzwerks.

Die Entscheidung für 6 Epochen und einen Batch-Size von 256 wurde getroffen, um eine angemessene Balance zwischen Trainingseffizienz und Modellleistung zu gewährleisten. Der Einsatz vom im Quellcode gezeigten TensorBoard-Aufruf bietet darüber hinaus eine effektive Möglichkeit, den Trainingsverlauf zu analysieren und etwaige Muster oder Probleme zu identifizieren.

# 4 Loss und Metriken

Um die Performance des Modells zu bewerten wurden mehrere Metriken verwendet.

Auf den Testdatensatz liefert das Modell eine Accuracy von 92,36%. Damit ist die zu Beginn gesetzte Vorgabe erreicht. Um des weiteren die Echtheit dieser Aussage zu überprüfen werden die Übereinstimmungen mit der Kappa-Statistik überprüft. Sie filtert zufällige Übereinstimmungen heraus und liefert einen Wert von -1 bis 1 als Rückgabewert. 1 steht dabei für die perfekte Übereinstimmung. Der vom Modell erreichte Kappa-Wert liegt bei 0.915 und kann als sehr gute bis perfekte Übereinstimmung interpretiert werden. Auch die Präzision, der Recall und der F1 Score des Modells sind sehr gut.

Zudem wird eine Confusion Matrix ausgegeben, die die wahren Label mit den vorhergesagten Labeln gegenüberstellt. Zu erkennen ist, dass Zahlen die bei undeutlicher Schrift sehr ähnliche Formen aufweisen am häufigsten verwechselt werden. So wird die tatsächliche Zahl 7 oft als 2 oder 9 interpretiert. Auch die im Datensatz mit 9

gelabelte Zahl wird verhältnismäßig oft als 4 oder 7 klassifiziert.

# 5 Ergebnisse und Bewertung

Aufgrund der Metriken bewertet sich das Modell angesichts der minimalen Trainingszeit und Parameter als äußerst erfolgreich. Verbesserungsmöglichkeiten ergeben sich jedoch bei der genaueren Unterscheidung von Zahlverwechslungen mit ähnlichen Formen wie 7, 2 und 9. Eine mögliche Optimierung, beispielsweise durch die Integration eines Filters zur Erkennung runder Strukturen, wurde getestet (`Zoom`-Funktion die Bilder auf doppelte Breite streckt um "Löcher"besser zu erkennen), jedoch stellte sich die damit verbundene längere Vorverarbeitungszeit unter Beachtung von Liste 1 als nicht umsetzbar heraus. Hiermit könnte die Genauigkeit noch verbessert werden, allerdings ist fraglich inwiefern die zu Beginn gesetzten Anforderungen hiermit erreicht werden können. Neuronale Netze gehen also auch lokal. Ob das zeitgemäß ist, ist eine andere Frage.

Zusätzliche Analysedaten können über den Tensorflow-Codeblock im Quellcode eingesehen werden.

# 6 Quellen

1. Long, L., Zeng, X. (2022). Beginning Deep Learning with TensorFlow: Work with Keras, MNIST Data Sets, and Advanced Neural Networks (1st ed. 2022.). Berkeley, CA: Apress.

2. https://www.kaggle.com/code/lailaelmahmoudi123/binary-classification-for-the-mnist-dataset

3. https://keras.io/api/layers/