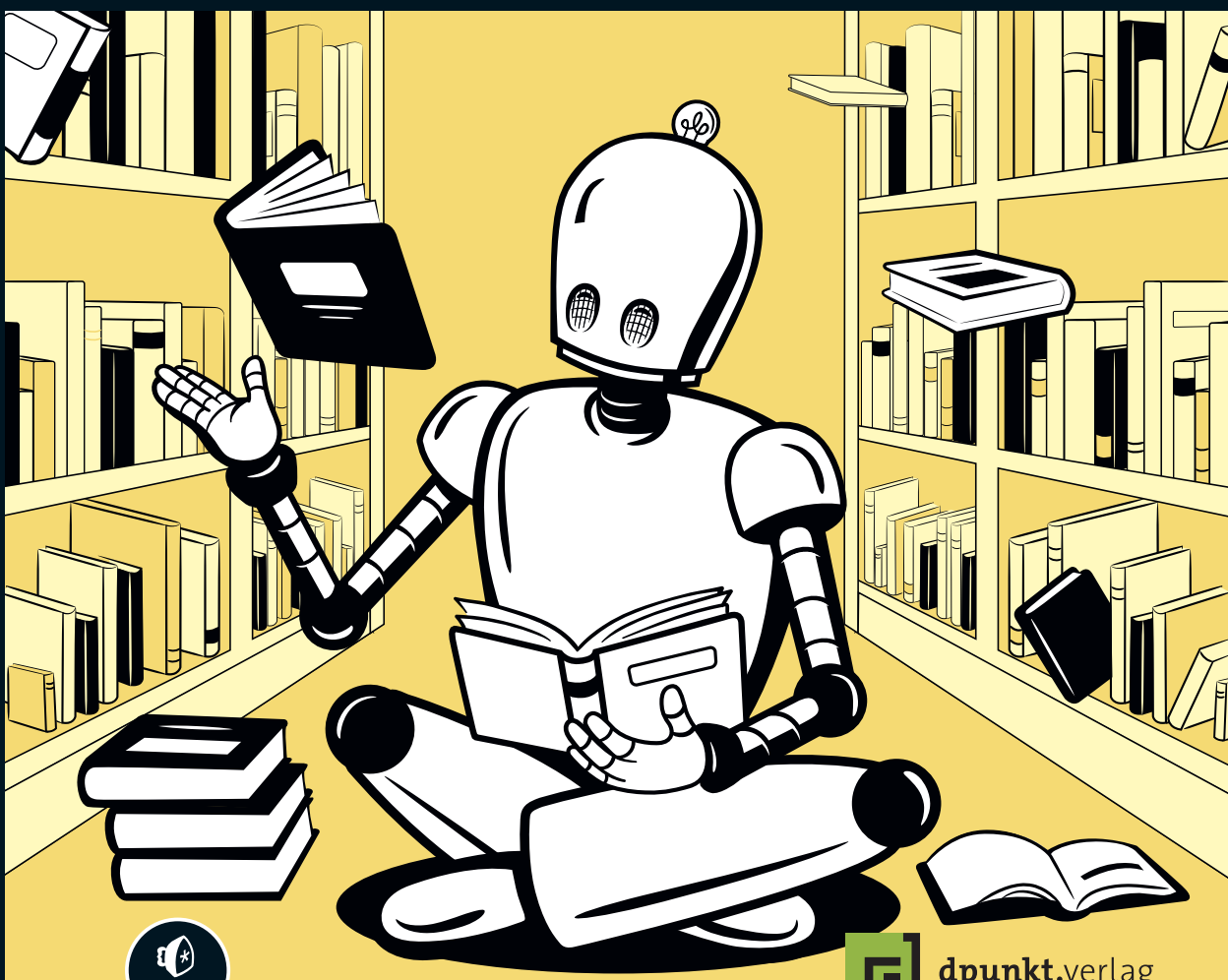
MACHINE LEARNING & KI

ZENTRALE KONZEPTE VERSTEHEN UND ANWENDEN

KOMPAKT

SEBASTIAN RASCHKA



no starch press

dpunkt.verlag

I Neuronale Netze und Deep Learning

1 Einbettungen, latenter Raum und Repräsentationen

Beim Deep Learning sind Begriffe wie *Einbettungsvektoren*, *Repräsentationen* und *latenter Raum* gebräuchlich. Was haben diese Konzepte gemeinsam und wie unterscheiden sie sich?

Auch wenn diese drei Begriffe oft synonym verwendet werden, können wir zwischen ihnen feine Unterscheidungen treffen:

- Einbettungsvektoren sind Repräsentationen von Eingabedaten, bei denen ähnliche Elemente nahe beieinanderliegen.
- Latente Vektoren sind Zwischenrepräsentationen von Eingabedaten.
- Repräsentationen sind codierte Versionen der ursprünglichen Eingabedaten.

Die folgenden Abschnitte untersuchen die Beziehung zwischen Einbettungen, latenten Vektoren und Repräsentationen. Außerdem erfahren Sie, wie sie jeweils im Kontext des maschinellen Lernens Informationen codieren.

1.1 Einbettungen

Einbettungsvektoren – kurz *Einbettungen* – codieren relativ hochdimensionale Daten in relativ niedrigdimensionale Vektoren.

Mithilfe von Einbettungsmethoden können wir einen kontinuierlichen dichten (nicht-dünnbesetzten) Vektor aus einer (dünnbesetzten) 1-aus-n-Codierung (englisch One-hot encoding) erzeugen. Die *1-aus-n-Codierung* ist eine Methode, um kategoriale Daten als binäre Vektoren darzustellen, wobei jede Kategorie auf einen Vektor abgebildet wird, der an der Position, die dem Index der Kategorie entspricht, eine 1, und an allen anderen Positionen eine 0 enthält. Damit ist sichergestellt, dass die kategorialen Werte so dargestellt werden, dass bestimmte Algorithmen für maschinelles Lernen sie verarbeiten können. Wenn wir zum Beispiel eine kategoriale Variable `Farbe` mit den drei Kategorien `Rot`, `Grün` und `Blau` haben, stellt die 1-aus-n-Codierung `Rot` als `[1, 0, 0]`, `Grün` als `[0, 1, 0]` und `Blau` als `[0, 0, 1]` dar. Diese 1-aus-n-codierten kategorialen Variablen lassen sich dann in kon-

tinuierliche Einbettungsvektoren abbilden, indem die gelernte Gewichtsmatrix einer Einbettungsschicht oder eines Moduls verwendet wird.

Einbettungsmethoden eignen sich auch für dichte Daten wie Bilder. Zum Beispiel können die letzten Schichten eines Convolutional Neural Networks (CNN) Einbettungsvektoren liefern, wie Abbildung 1–1 veranschaulicht.

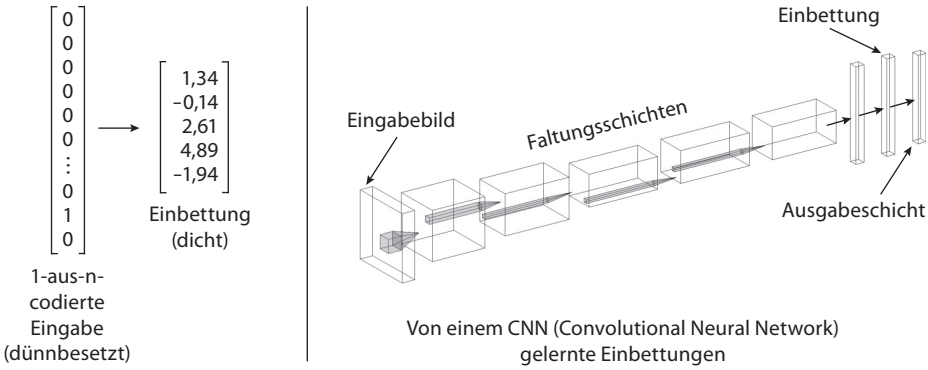


Abb. 1–1 *Eine Eingabeeinbettung (links) und eine Einbettung von einem neuronalen Netz (rechts)*

Um technisch korrekt zu sein, könnten alle Ausgaben der Zwischenschicht eines neuronalen Netzes Einbettungsvektoren liefern. Je nach Trainingsziel kann auch die Ausgabeschicht nützliche Einbettungsvektoren erzeugen. Der Einfachheit halber assoziiert das Convolutional Neural Network in Abbildung 1–1 die vorletzte Schicht mit Einbettungen.

Es ist möglich, dass Einbettungen eine höhere oder niedrigere Anzahl von Dimensionen haben als die ursprüngliche Eingabe. Mithilfe von Einbettungsmethoden für extreme Ausdrücke lassen sich beispielsweise Daten in zweidimensionale dichte und kontinuierliche Darstellungen für Visualisierungszwecke und Clustering-Analysen codieren, wie Abbildung 1–2 zeigt.

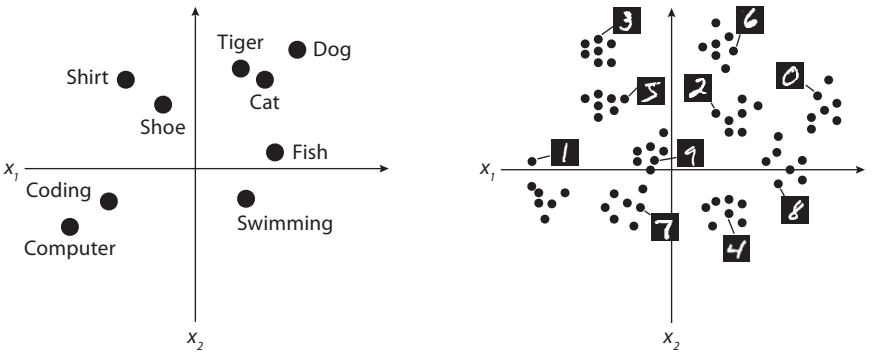


Abb. 1–2 *Abbildung von Wörtern (links) und Bildern (rechts) auf einen zweidimensionalen Merkmalsraum*

Zu den grundlegenden Eigenschaften von Einbettungen gehört, dass sie *Abstand* oder *Ähnlichkeit* codieren. Das bedeutet, dass Einbettungen die Semantik der Daten so erfassen, dass ähnliche Eingaben im Einbettungsraum nahe beieinanderliegen.

Für Leser, die an einer formaleren Erklärung mittels mathematischer Terminologie interessiert sind, sei erwähnt, dass eine Einbettung eine injektive und strukturerhaltende Abbildung zwischen einem Eingaberaum X und dem Einbettungsraum Y ist. Dies impliziert, dass ähnliche Eingaben an nahe beieinanderliegenden Punkten innerhalb des Einbettungsraums liegen, was man als »strukturerhaltende« Eigenschaft der Einbettung ansehen kann.

1.2 Latenter Raum

Latenter Raum wird in der Regel synonym mit *Einbettungsraum* verwendet, das heißt dem Raum, in den Einbettungsvektoren abgebildet werden.

Ähnliche Elemente können im latenten Raum nahe beieinanderliegen, was jedoch keine strikte Voraussetzung ist. Im weiteren Sinne kann man sich den latenten Raum als jeden Merkmalsraum vorstellen, der Features – oftmals komprimierte Versionen der ursprünglichen Eingabefeatures – enthält. Diese latenten Raumfeatures können von einem neuronalen Netzwerk erlernt werden, beispielsweise einem Autoencoder, der Eingabebilder rekonstruiert, wie Abbildung 1–1 zeigt. Diese latenten Eingabefeatures können von einem neuronalen Netz gelernt werden, beispielsweise von einem Autoencoder, der Eingabebilder rekonstruiert, wie Abbildung 1–3 zeigt.

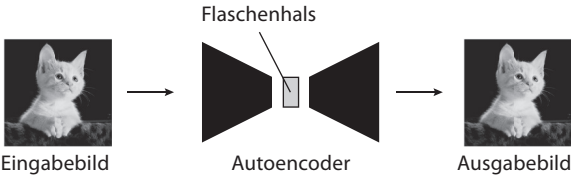


Abb. 1–3 *Ein Autoencoder, der das Eingabebild rekonstruiert*

Der Flaschenhals in Abbildung 1–3 repräsentiert eine kleine Zwischenschicht des neuronalen Netzes, die das Eingabebild in eine Repräsentation geringerer Dimensionen codiert. Den Zielraum dieser Abbildung kann man sich als latenten Raum vorstellen. Das Trainingsziel des Autoencoders besteht darin, das Eingabebild zu rekonstruieren, das heißt, den Abstand zwischen den Eingabe- und Ausgabebildern zu minimieren. Um das Trainingsziel zu optimieren, kann der Autoencoder lernen, die codierten Features von ähnlichen Eingaben (zum Beispiel Bilder von Katzen) im latenten Raum nahe nebeneinander zu platzieren, dabei nützliche Einbettungen von Vektoren zu erstellen, wobei ähnliche Eingaben im Einbettungs- (latenten) Raum nahe beieinanderliegen.

1.3 Repräsentation

Eine *Repräsentation* ist eine codierte Form und typischerweise eine Zwischenform einer Eingabe. Zum Beispiel ist ein Einbettungsvektor bzw. Vektor im latenten Raum eine Darstellung der Eingabe, wie oben erläutert. Allerdings können Darstellungen auch mit einfacheren Prozeduren erzeugt werden. Zum Beispiel lassen sich 1-aus-n-codierte Vektoren als Repräsentationen einer Eingabe betrachten, wie bereits oben erwähnt. Allerdings lassen sich Repräsentationen auch durch einfachere Verfahren erzeugen. So werden zum Beispiel 1-aus-n-codierte Vektoren als Repräsentationen einer Eingabe betrachtet.

Der Grundgedanke besteht darin, dass die Repräsentation einige wesentliche Features oder Eigenschaften der ursprünglichen Daten erfasst, um sie weiter analysieren zu können.

1.4 Übungen

1. Angenommen, wir trainieren ein Netz mit fünf konvolutionalen Schichten, gefolgt von drei vollständig verbundenen Schichten, ähnlich dem AlexNet (*https://en.wikipedia.org/wiki/AlexNet*), wie in Abbildung 1–4 veranschaulicht.

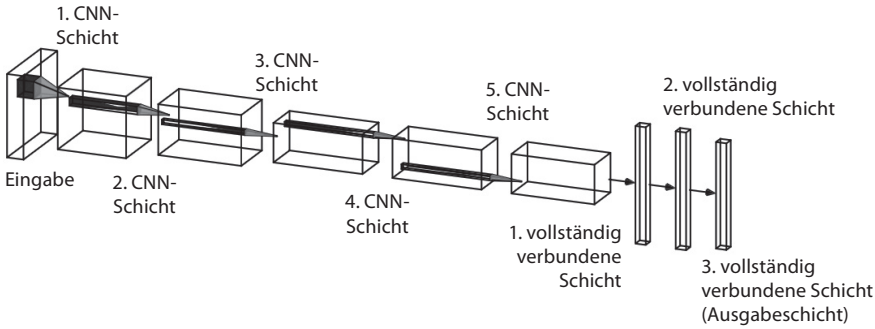


Abb. 1–4 *Eine Veranschaulichung von AlexNet*

   Diese vollständig verbundenen Schichten kann man sich als zwei verdeckte Schichten und eine Ausgabeschicht in einem mehrschichtigen Perzeptron vorstellen. Welche Schichten dieses neuronalen Netzes lassen sich nutzen, um nützliche Einbettungen zu erzeugen? Interessierte Leser finden weitere Details zur Architektur und Implementierung von AlexNet in der Originalveröffentlichung von Alex Krizhevsky, Ilya Sutskever und Geoffrey Hinton.

2. Nennen Sie einige Typen von Eingaberepräsentationen, die keine Einbettungen sind.

1.5 Referenzen

- Die Architektur und Implementierung von AlexNet wird ursprünglich in folgendem Paper beschrieben: Alex Krizhevsky, Ilya Sutskever und Geoffrey Hinton, »ImageNet Classification with Deep Convolutional Neural Networks« (2012), *https://papers.nips.cc/paper/4824-imagenet-classification-with-deep-convolutional-neural-networks*.

2 Selbstüberwachtes Lernen

Was ist selbstüberwachtes Lernen, wann ist es nützlich und wie sehen die Hauptansätze aus, um es zu implementieren?

Selbstüberwachtes Lernen ist eine Vortrainingsprozedur, die es neuronalen Netzen ermöglicht, große, ungelabelte Datensätze in überwachter Art und Weise zu nutzen. Dieses Kapitel vergleicht selbstüberwachtes Lernen mit Transferlernen, einer verwandten Methode zum Vortrainieren von neuronalen Netzen, und erörtert die praktischen Anwendungen von selbstüberwachtem Lernen. Schließlich skizziert es die wichtigsten Kategorien von selbstüberwachtem Lernen.

2.1 Selbstüberwachtes Lernen vs. Transferlernen

Selbstüberwachtes Lernen ist mit dem Transferlernen verwandt, einer Technik, bei der ein Modell, das für eine bestimmte Aufgabe vortrainiert worden ist, als Ausgangspunkt für ein Modell für eine zweite Aufgabe wiederverwendet wird. Nehmen wir zum Beispiel an, dass wir einen Bildklassifikator trainieren wollen, um Vogelarten zu klassifizieren. Beim Transferlernen würden wir ein CNN (Convolutional Neural Network) auf dem ImageNet-Datensatz trainieren, einem großen, gelabelten Bilddatensatz mit vielen verschiedenen Kategorien, einschließlich verschiedener Objekte und Tiere. Nach dem Vortraining mit dem allgemeinen ImageNet-Datensatz wird das trainierte Modell mit dem kleineren, spezifischeren Zieldatensatz trainiert, der die interessierenden Vogelarten enthält. (Oftmals müssen wir nur die klassenspezifische Ausgabeschicht ändern, können ansonsten aber das vortrainierte Netz unverändert übernehmen.)

Abbildung 2–1 veranschaulicht den Ablauf beim Transferlernen.

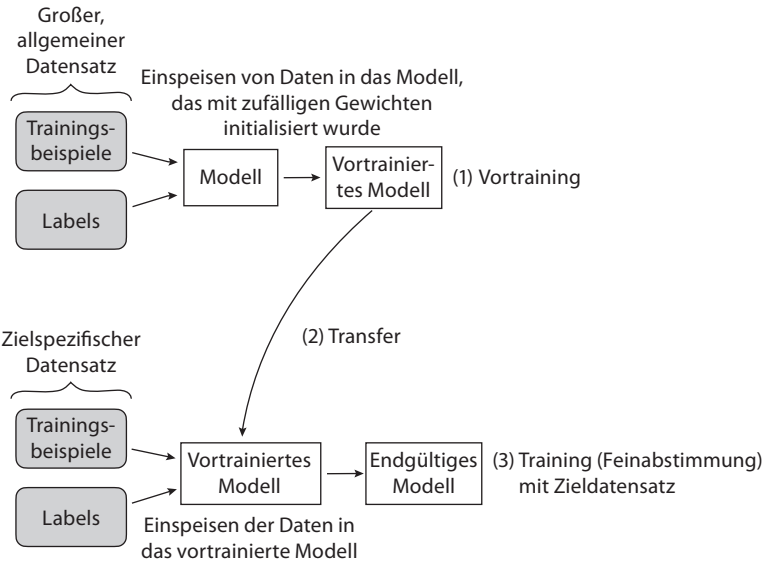


Abb. 2–1 *Vortraining mit konventionellem Transferlernen*

Selbstüberwachtes Lernen ist ein alternativer Ansatz zum Transferlernen, bei dem das Modell nicht mit gelabelten Daten, sondern mit ungelabelten Daten vortrainiert wird. Wir betrachten einen ungelabelten Datensatz, für den wir keine Label-Informationen haben, und suchen dann nach einer Möglichkeit, Labels aus der Struktur des Datensatzes zu erhalten, um eine Vorhersageaufgabe für das neuronale Netz zu formulieren, wie Abbildung 2–2 zeigt. Diese Aufgaben für das selbstüberwachte Training nennt man auch *Voraufgaben*.

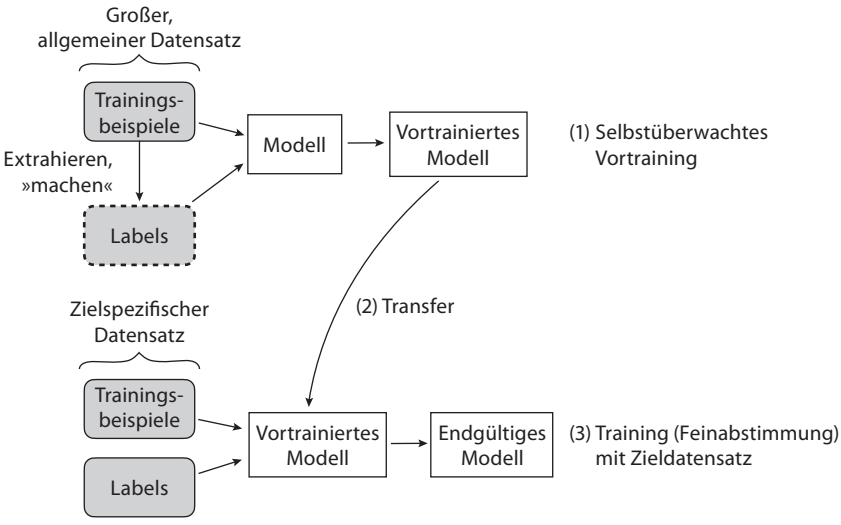


Abb. 2–2 *Vortraining mit selbstüberwachtem Lernen*

Der Hauptunterschied zwischen Transferlernen und selbstüberwachtem Lernen liegt in der Art und Weise, wie wir die Labels in Schritt 1 der Darstellungen von Abbildung 2–1 und Abbildung 2–2 erhalten. Beim Transferlernen gehen wir davon aus, dass die Labels zusammen mit dem Datensatz bereitgestellt werden. In der Regel werden die Labels manuell von Label-Experten den Daten zugeordnet. Beim selbstüberwachten Lernen lassen sich die Labels direkt aus den Trainingsbeispielen ableiten.

Eine Aufgabe des selbstüberwachten Lernens könnte eine Vorhersage fehlender Wörter im Kontext der Verarbeitung natürlicher Sprache sein. Zum Beispiel können wir bei dem Satz »Draußen ist es schön und sonnig« das Wort »sonnig« ausmaskieren, dem Netz die Eingabe »Draußen ist es schön und [MASKE]« einspeisen und das Netz das fehlende Wort an der Position »[MASKE]« vorhersagen lassen. In ähnlicher Weise könnten wir in einem Computer-Vision-Kontext Bildausschnitte entfernen und das neuronale Netz die Lücken füllen lassen. Dies sind lediglich zwei Beispiele für Aufgaben des selbstüberwachten Lernens; es gibt viele weitere Methoden und Paradigmen für diese Art des Lernens.

Zusammenfassend lässt sich sagen, dass man selbstüberwachtes Lernen bei der Voraufgabe als Repräsentationslernen betrachten kann. Wir können das vorab trainierte Modell verwenden, um es für die Zielaufgabe (auch bekannt als die *Downstream*-Aufgabe) zu optimieren.

2.2 Ungelabelte Daten nutzen

Große Architekturen neuronaler Netze benötigen große Mengen an gelabelten Daten, um eine gute Leistung und Generalisierung zu erzielen. Für viele Problembereiche haben wir jedoch keinen Zugang zu großen, gelabelten Datensätzen. Beim selbstüberwachten Lernen können wir ungelabelte Daten nutzen. Daher ist selbstüberwachtes Lernen beim Arbeiten mit großen neuronalen Netzen und mit einer begrenzten Menge von gelabelten Trainingsdaten höchstwahrscheinlich nützlich.

Transformer-basierte Architekturen, die die Grundlage der LLMs und Vision Transformer bilden, erfordern bekanntermaßen selbstüberwachtes Lernen für das Vortraining, um gute Leistungen zu erzielen.

Für kleine Modelle von neuronalen Netzen wie zum Beispiel mehrschichtige Perzeptrons mit zwei oder drei Schichten wird selbstüberwachtes Lernen in der Regel weder als nützlich noch als notwendig erachtet.

Selbstüberwachtes Lernen ist auch beim herkömmlichen maschinellen Lernen mit nichtparametrischen Modellen wie baumbasierten Random Forests oder Gradient Boosting nicht sinnvoll. Konventionelle baumbasierte Methoden besitzen keine feste Parameterstruktur (im Gegensatz zum Beispiel zu den Gewichtsmatrizen). Daher sind konventionelle baumbasierte Methoden nicht zum Transferlernen fähig und mit selbstüberwachtem Lernen nicht kompatibel.

2.3 Selbstvorhersage und kontrastives selbstüberwachtes Lernen

Es gibt zwei Hauptkategorien des selbstüberwachten Lernens: Selbstvorhersage und kontrastives selbstüberwachtes Lernen. Bei der *Selbstvorhersage*, die in Abbildung 2–3 dargestellt ist, ändern oder verbergen wir normalerweise Teile der Eingabe und trainieren das Modell, um die ursprünglichen Eingaben zu rekonstruieren. Hierfür verwendet man zum Beispiel eine Störungsmaske, die bestimmte Pixel in einem Bild verschleiert.

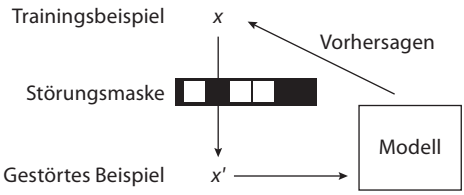


Abb. 2–3 *Selbstvorhersage nach dem Anwenden einer Störungsmaske*

Ein klassisches Beispiel ist ein entrauschender Autoencoder, der lernt, Rauschen aus einem Eingabebild zu entfernen. Als Alternative betrachten wir einen maskierten Autoencoder, der die fehlenden Teile eines Bildes rekonstruiert, wie Abbildung 2–4 zeigt.

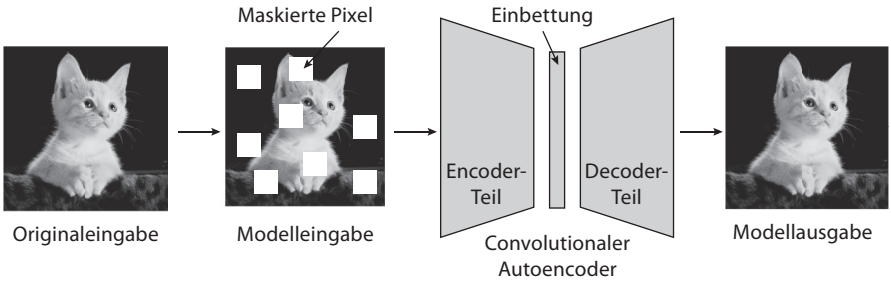


Abb. 2–4 *Ein maskierter Autoencoder, der ein maskiertes Bild rekonstruiert*

Methoden zur Selbstvorhersage bei fehlender (maskierter) Eingabe werden häufig auch im Zusammenhang mit der Verarbeitung natürlicher Sprache eingesetzt. Viele generative LLMs, wie zum Beispiel GPT, werden auf eine Vorhersageaufgabe für das nächste Wort trainiert (Kapitel 14 und 17 gehen ausführlicher auf GPT ein). Hier speisen wir das Netz mit Textfragmenten, aus denen es das nächste Wort in der Sequenz vorhersagen muss (wie ich in Kapitel 17 näher erläutern werde).

Beim *kontrastiven selbstüberwachten Lernen* trainieren wir das neuronale Netz, sodass es einen Einbettungsraum lernt, in dem ähnliche Eingaben nahe beieinander und unähnliche Eingaben weit auseinanderliegen. Mit anderen Worten: Wir trainieren das Netz, um Einbettungen zu erzeugen, die den Abstand zwischen

ähnlichen Trainingseingaben minimieren und den Abstand zwischen unähnlichen Trainingsbeispielen maximieren.

Kontrastives Lernen möchte ich nun anhand konkreter Beispiele erörtern. Angenommen, wir haben einen Datensatz, der aus zufälligen Tierbildern besteht. Zunächst zeichnen wir ein zufälliges Bild einer Katze (das Netz kennt das Label nicht, weil wir davon ausgehen, dass der Datensatz ungelabelt ist). Dann wird dieses Katzenbild erweitert, beschädigt oder gestört, indem eine zufällige Rauschschicht hinzugefügt und unterschiedlich beschnitten wird, wie Abbildung 2–5 zeigt.

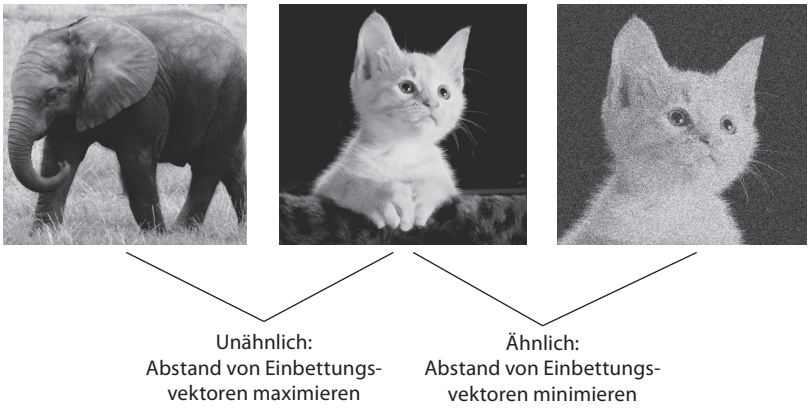


Abb. 2–5 *Bildpaare, wie sie beim kontrastiven Lernen auftreten*

Das gestörte Katzenbild in dieser Abbildung zeigt immer noch dieselbe Katze, also soll das Netz einen ähnlichen Einbettungsvektor erzeugen. Außerdem betrachten wir ein zufälliges Bild aus der Trainingsmenge (zum Beispiel einen Elefanten, aber auch hier kennt das Netz das Label nicht).

Für das Katzen-Elefanten-Paar soll das Netz unähnliche Einbettungen erzeugen. Auf diese Weise zwingen wir das Netz implizit dazu, den Kerninhalt des Bildes zu erfassen und gleichzeitig gegenüber kleinen Unterschieden und Rauschen einigermaßen agnostisch zu sein. Zum Beispiel ist die einfachste Form eines kontrastiven Verlustes die L_2-Norm (euklidischer Abstand) zwischen den Einbettungen, die das Modell M(·) erzeugt. Beispielsweise können wir die Modellgewichte aktualisieren, um den Abstand `||M(cat) - M(cat?)||`$_2$ zu verringern und den Abstand `||M(cat) - M(elephant)||`$_2$ zu vergrößern.

Abbildung 2–6 fasst das zentrale Konzept des kontrastiven Lernens für das Szenario mit dem gestörten Bild zusammen. Das Modell ist zweimal abgebildet, was als *siamesischer Netzaufbau* bekannt ist. Im Wesentlichen wird dasselbe Modell in zwei Instanzen verwendet: erstens, um die Einbettung für das ursprüngliche Trainingsbeispiel zu generieren, und zweitens, um die Einbettung für die gestörte Version des Beispiels zu erzeugen.

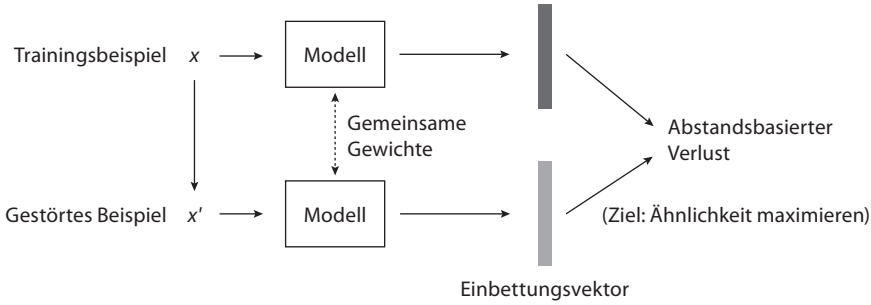


Abb. 2–6 *Kontrastives Lernen*

Dieses Beispiel skizziert den Grundgedanken des kontrastiven Lernens, von dem es aber viele Untervarianten gibt. Im Großen und Ganzen können wir diese in kontrastive Methoden für *Muster* und kontrastive Methoden für *Dimensionen* kategorisieren. Das Elefanten-Katzen-Beispiel in Abbildung 2–6 veranschaulicht eine beispielhafte kontrastive Methode, bei der wir das Lernen von Einbettungen in den Mittelpunkt stellen und die Abstände zwischen den Trainingspaaren maximieren. Bei *dimensionsbezogenen* kontrastiven Ansätzen konzentrieren wir uns hingegen darauf, nur bestimmte Variablen in den Einbettungsrepräsentationen ähnlicher Trainingspaare nahe beieinander erscheinen zu lassen, während der Abstand anderer maximiert wird.

2.4 Übungen

1. Wie könnte man selbstüberwachtes Lernen auf Videodaten anwenden?
2. Lässt sich selbstüberwachtes Lernen für tabellarische Daten verwenden, die als Zeilen und Spalten dargestellt werden? Wenn ja, wie könnte man dies angehen?

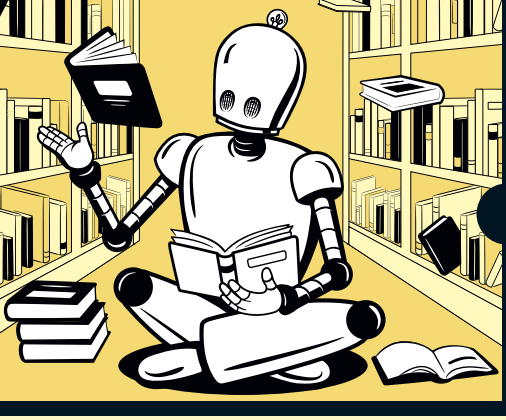
2.5 Referenzen

- Mehr über den ImageNet-Datensatz finden Sie unter: *https://en.wikipedia.org/wiki/ImageNet*.
- Ein Beispiel für eine kontrastive selbstüberwachte Lernmethode: Ting Chen et al., »A Simple Framework for Contrastive Learning of Visual Representations« (2020), *https://arxiv.org/abs/2002.05709*.
- Ein Beispiel für eine dimensionsorientierte kontrastive Methode: Adrien Bardes, Jean Ponce und Yann LeCun, »VICRegL: Self-Supervised Learning of Local Visual Features« (2022), *https://arxiv.org/abs/2210.01571*.
- Wenn Sie vorhaben, selbstüberwachtes Lernen in der Praxis einzusetzen: Randall Balestriero et al., »A Cookbook of Self-Supervised Learning« (2023), *https://arxiv.org/abs/2304.12210*.

- Ein Paper, das eine Methode des Transferlernens und des selbstüberwachten Lernens für relativ kleine mehrschichtige Perzeptrons auf tabellarischen Datensätzen vorschlägt: Dara Bahri et al., »SCARF: Self-Supervised Contrastive Learning Using Random Feature Corruption« (2021), *https://arxiv.org/abs/2106.15147*.
- Ein zweites Paper, das eine derartige Methode vorschlägt: Roman Levin et al., »Transfer Learning with Deep Tabular Models« (2022), *https://arxiv.org/abs/2206.15306*.

Inhaltsverzeichnis

Teil V Vorhersageperformance und Modellevaluierung



- SCHLIESST DIE LÜCKE ZWISCHEN GRUNDLAGEN UND PROFIWISSEN
- EINFACHE, PRÄGNANTE ERKLÄRUNGEN ZU WICHTIGEN UND AKTUELLEN THEMEN
- MIT ÜBUNGSAUFGABEN SOWIE CODEBEISPIELEN AUF GITHUB

Sie verfügen bereits über Grundkenntnisse zu maschinellem Lernen und künstlicher Intelligenz, haben aber viele Fragen und wollen tiefer in wesentliche und aktuelle Konzepte eintauchen? ML- und KI-Experte Sebastian Raschka greift in diesem Buch die wichtigsten Schlüsselfragen auf und liefert sowohl prägnante als auch einfach verständliche Erklärungen zu komplexen und fortgeschrittenen Themen wie Deep Learning, Überanpassung, Self-Supervised Learning, generative KI, Computer Vision, Natural Language Processing und Modellevaluierung.

Viele Beispiele, anschauliche Illustrationen und praktische Übungsaufgaben helfen Ihnen dabei, das Erlernte nicht nur schnell zu verstehen, sondern auch praktisch umzusetzen. Dabei werden weder fortgeschrittene Mathematik- noch Programmierkenntnisse vorausgesetzt – wer tiefer in den Code eintauchen will, findet jedoch im kostenlosen Zusatzmaterial einige Codebeispiele.

Aus dem Inhalt:

- Umgang mit verschiedenen Zufallsquellen beim Training neuronaler Netze
- Unterscheidung zwischen Encoder- und Decoder-Architekturen in großen Sprachmodellen (LLMs)
- Verringerung von Überanpassung durch Daten- und Modellmodifikationen
- Konstruktion von Konfidenzintervallen für Klassifizierer und Optimierung von Modellen mit begrenzten gelabelten Daten
- Wählen zwischen verschiedenen Multi-GPU-Trainingsparadigmen und verschiedenen Arten von generativen KI-Modellen
- Verstehen von Performancemetriken für die Verarbeitung natürlicher Sprache

ÜBER DEN AUTOR

Sebastian Raschka ist Forscher für maschinelles Lernen und Ausbilder für KI bei Lightning AI. Er ist Autor der Bestseller »Python Machine Learning« und »Machine Learning with PyTorch and Scikit-Learn«. Erfahren Sie mehr über seine Projekte unter *https://sebastianraschka.com*.

no starch press

€ 34,90 (D)

Gedruckt in Deutschland
Mineralölfreie Druckfarben
Zertifiziertes Papier

ISBN 978-3-98889-031-3