Masterseminar AI "Trends in Deep Learning"

Sommersemester 2023

Heinrich Jasper, Volker Göhler

TU Bergakademie Freiberg

28. März 2023

Verlauf

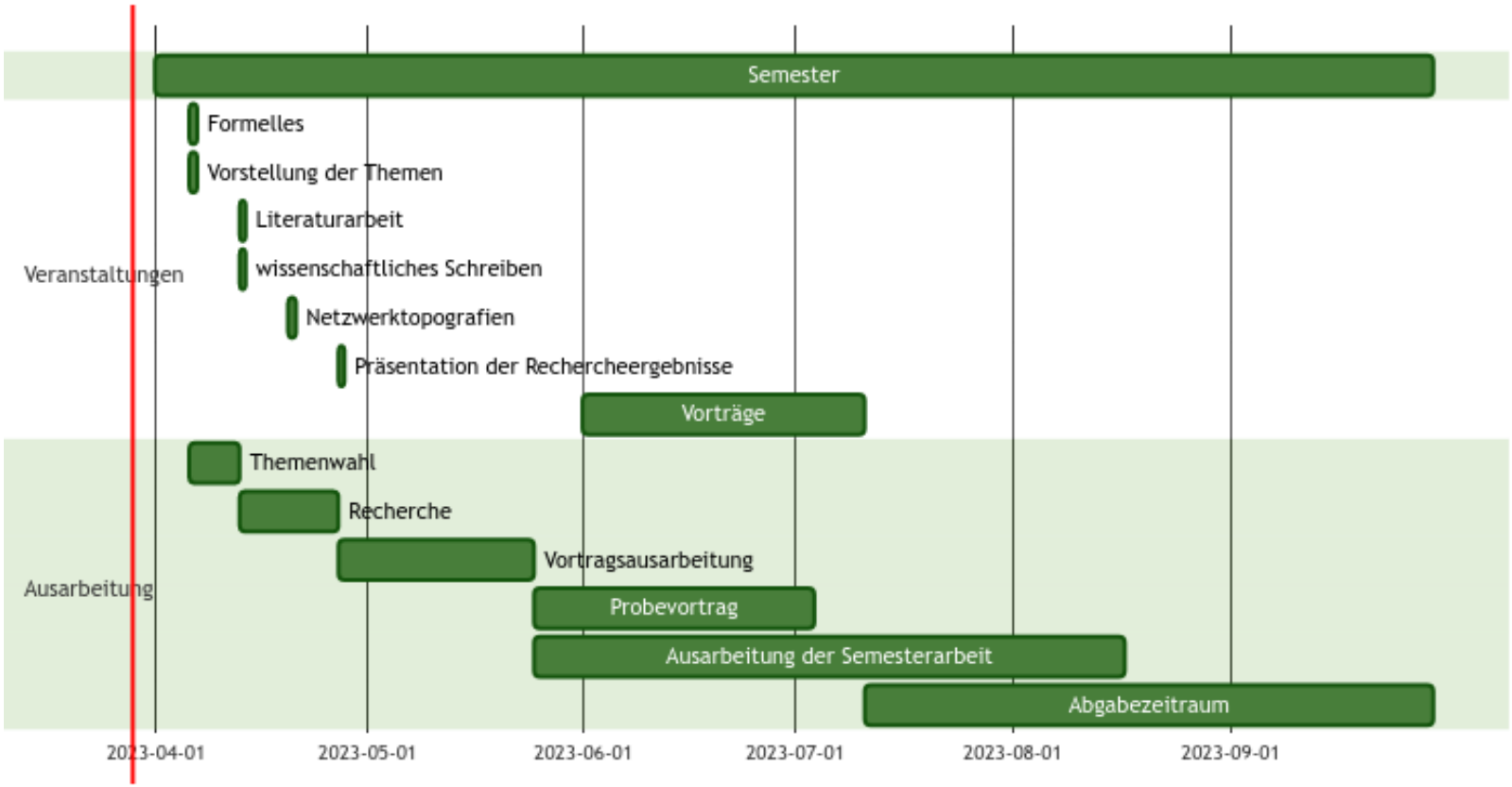

Abbildung 1: Semesterverlauf (Änderungen vorbehalten)

Leistungsnachweis

- ein wissenschaftlicher Vortrag von ca. 45 min Dauer
- eine Seminararbeit mit wissenschaftlichem Anspruch im Umfang von ca. 12 Seiten
- Mitarbeit am Seminar (seien Sie anwesend und stellen Sie Fragen!)

Themen

- Sie wählen sich ein Thema (siehe Opal)
- Sie führen eine Literaturrecherche zu dem Thema durch um State of the Art Research Paper zu finden
- Sie stellen die Ergebnisse Ihrer Literaturrecherche vor
- Und arbeiten dann einen Vortrag aus indem der State of the Art kritisch vorgestellt wird
- Abschließend schreiben Sie eine Seminararbeit zu SotA, ihrer Literaturrecherche und Ihrer Kritik

Vortrag

- deutsch / englisch
- Termine für die Vorträge werden im Mai bekannt gegeben
- melden Sie sich ausreichend vorher wenn Sie verhindert sind
- Seien Sie bitte alle zu allen Vorträgen da
- Ein Testvortrag zur Qualitätssicherung ist Pflicht
- Vereinbaren Sie bitte einen Termin mit Herrn Göhler, mindestens eine Woche vorher
- Vortrag ca. 35 min Dauer, 10 min Diskussion

Seminararbeit

- eine Arbeit mit wissenschaftlichem Anspruch
- ca. 12 Seiten
- mindestens zwei weitere Primärquellen, die das Thema einordnen
- Achten Sie auf korrekte Form der Arbeit, insbesondere auf Referenzen und Zitationen
- Kopieren Sie nicht! Plagiate sind ein ernster Verstoß!
- Abgabe bis Ende September (Sagen Sie Bescheid wenn sich Ihre Abgabe verspätet!)

Sonstiges

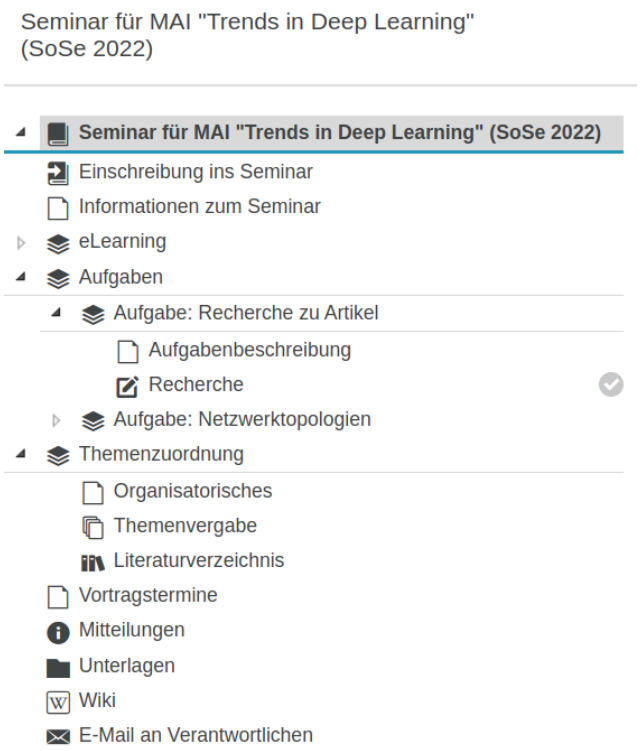

Abbildung 2: Opal Table of Contents (Ihre Ansicht kann sich geringfügig unterscheiden!)

- Ihre Opalanmeldung am Kurs ist notwendig
- Alle Abgaben über die entsprechenden Komponenten im Opal
- Kommunikation über Opal

Fragen zum Formellen?

Themenübersicht

- wählen Sie sich ein Thema (im Opal) bis nächsten Donnerstag aus
  - First come first served, keine Doppelvergaben
  - Wenn Sie selber eine Idee haben, was Sie gern im Bereich DNN untersuchen möchten, dann kontaktieren Sie Herrn Göhler
- Sie können das Thema auch variieren sofern Sie am SotA bleiben (Besprechen Sie das mit Herrn Göhler)
- Am Ende der Recherche bekommen Sie einen Paper passend zum Thema (sollten Sie den bei der Recherche nicht gefunden haben)
- Bei weiteren Fragen kontaktieren Sie ebenso Herrn Göhler

Dataset Poisoning und Gegenmassnahmen, SotA

Dataset Poisoning beschreibt einen Angriff auf ein Neuronales Netz indem Daten in der Trainingsmenge korumpiert werden, um das Ergebniss des Netzes in eine vom Angreifer gewünschte Richtung zu verschieben. Stellen sie den State of the Art dar.

Adversarial Attacks auf Text 2 Bild Generatoren

Aus Text generierte Bilder sind eine schnell greifbare Anwendung, die im letzten Jahr produktionsreife Modelle ergeben hat. Beim Input haben Nutzer viele (textuelle, aber auch grafische) Möglichkeiten. Adversarial Attacks manipulieren den Input eines Netztes um eine vom Nutzer gewünschte Reaktion hervorzurufen, die sich von der normalerweise gemachten unterscheidet.

Neural Programming, Sota

Natürliche und künstliche Neuronale Systeme sind effiziente Computer, die auf eine andere Weise daten prozessieren als halbleiter basierte Systeme. Es gibt Bemühungen native Programmiersprachen für Neuronale Systeme zu etablieren. Stellen Sie den SotA dar.

Training Data Extraction

Trainierte Neuronale Netze werden oft als Blackbox angesehen. Dies stimmt nur bedingt. Es existiert eine größere Menge an Möglichkeiten aus z.B. Klassifizierungsnetzwerken Trainingsdaten teilweise zu rekonstruieren. Stellen Sie den State of the Art dar.

Text to 3D

In den letzten Jahren hat es einige Fortschritte in der Bildgenerierung gegeben. Meist wurden 2D Bilder erstellt, da aber auch ein breites Anwendungsfeld im 3D besteht gibt es auch Generatoren die dieses Feld bedienen können. Stellen Sie den State of the Art dar und zeigen Sie Anwendungen.

Spiking Neural Networks, SotA

SNNs sind näher an den biologischen Neuron und stellen zusätzlich zeitliche Abläufe mit dar. Zeigen Sie Anwendungsgebiete und den SotA.

Text to Speech Synthesizers

Bereits seit den 90er Jahren beschäftigt man sich damit Texte maschinell vorzulesen. Fortschritte wurden in den letzten Jahren gerade bei natürlicher Betonung gemacht. Stellen Sie den State of the Art im Zusammenhang mit neuronalen Netzen dar.

Diffusion Models, SotA

Bei der Bildgenerierung aus Texten hat sich in den letzten beiden Jahren ein großer Fortschritt eingestellt. Stellen Sie die verwendeten Diffusion Modelle dar und zeigen Sie weitere Anwendungsbereiche.

Self Training on unlabeled Data, SotA

Gelabelte Trainingsbeispiele werden zwingend von Neuronalen Netzen (teils in großer Zahl) benötigt. Das labeln wird meist manuell durchgeführt und ist langwierig, daher ist es von Vorteil wenn sich Netze von ungelabelten Daten Trainieren lassen. Stellen Sie den State of the Art dar und skizieren Sie Anwendungszenarien.

Generative Pre-Trained Transformers, SotA

GPT's werden zur automatisierten Textgenierung verwendet. ChatGPT und GPT4.0 von OpenAI sind aktuell die Spitzenmodelle. Stellen Sie den SotA dar und zeigen Sie Limitationen und Anwendungsmöglichkeiten.

Themenauswahl im Opal

Abbildung 3: Question Mark Icon By PlatformerKing - Own work, CC BY-SA 4.0 Link

- entscheiden Sie sich bis nächsten Donnerstag
- bei Fragen jetzt fragen oder Email schreiben
- beginnen Sie dann mit der Recherche
- Ihre Ergebnisse der Recherchen werden wir am 27.04. vergleichen

Rechercheaufgabe

Recherchieren Sie zu **AI die Minecraft spielen kann**.

- Finden Sie heraus wer die Forschung gemacht hat (Person/Forschungseinrichtung)
- Wie lauten die Titel der ursprünglichen Researchpaper?
- Wie sind Sie bei der Recherche vorgegangen?
- Hatten Sie andere Herausforderungen?
- Wieviele Ergebnisse gibt es verteilt über die Jahre (Histogram)
- Wie ist das Verhältniss von Zweitquellen (Presse, Blogs etc.) zu originaler Forschung (Journal und Conference Papers)?

Hinweise

- Geben Sie bis Mittwoch nächste Woche (im Opal Aufgaben->Aufgabe: Recherche zu Artikel->Abgabe der Recherchen) Ihre Antworten zu den obigen Fragen ab
- Wir besprechen die Ergebnisse am kommenden Donnerstag
- Kurze Antworten und Stichpunkte reichen, Schreiben Sie nicht mehr als eine Seite, aber referenzieren Sie Ihre Quellen korrekt

Fragen?