

Synthetic Content for Probe-Resistant Proxies

Zwischenbericht | Call 16 | Stipendium ID 5900

Lizenz: CC-BY



Inhalt

1	Einle	eitung	3
2	Stat	US	3
	2.1 2.2	Meilenstein 1 – Erhebung des Forschungsstandes	
3	Zusa	ammenfassung Planaktualisierung	5



1 Einleitung

Vorab will ich darauf eingehen, warum es zu gröberen Verzögerungen während meines Projektes kam. Während die ersten beiden Meilensteine wie zeitlich geplant abgeschlossen waren, verzögerte sich die Entwicklung des geplanten Frameworks im Zuge der Masterarbeit enorm durch die OpenAI Inc und dem API-Freigabeverfahren für ihr autoregressives Sprachmodell GPT-3, sowie zu DALL-E 2, einem Modell, dass aus einem Text fotorealistische Bilder generieren kann. Im Vorfeld der Arbeit wurde mir sowohl durch Kontakte über das Tor Project als auch über Verbindungen durch die Universität in Michigan seitens der OpenAI Inc, Zugang zu Ihren programmatischen Schnittstellen für GPT-3 und im Laufe der Monate ebenso zu DALL-E 2 zugesichert. Zusätzlich verkündete OpenAI Ende 2021 ¹an, dass der Zugang zu der API für GPT-3 ab sofort ohne Warteliste erfolgen wird.

Jedoch wurde selbst nach wiederholtem Anfragen kein API-Key zur Verfügung gestellt, wie ursprünglich versprochen. Stattdessen wurde ich stets damit vertröstet, dass sie gerade mit Anfragen überflutet werden und sie um Verständnis bitten.

Das im Zuge des Projekts entwickelte Framework baut stark auf die Unterstützung durch GPT-3 auf, um den synthetischen Inhalt zu generieren.

Es bestehen zwar genügend Alternativen, wie das GPT-NeoX Model von EleutherAl ²oder das Model Bloom von BigScience³, jedoch müssten beide Systeme selbst aufgesetzt und betrieben werden, was zu immens hohen Kosten führt, da das erstere Modell eine Server Instanz mit mindestens 45GB GPU VRAM und letzteres eine Instanz mit mindestens 352 GB RAM benötigen würde. Ziel des Frameworks ist jedoch das Generieren von synthetischen Webseiten möglichst Userfreundlich und mit geringem Aufwand zu ermöglichen, wodurch die Alternativen keine attraktiven Lösungen sind.

Obwohl sämtliche Meilensteine wie geplant vor der Einreichung des Zwischenberichts bereits vor einigen Monaten abgeschlossen wurden, verzögerte sich das Erstellen des Berichts aufgrund der oben genannten Gründe, da die Fertigstellung des Projekts für einige Monate in der Schwebe lag. Ich wollte diesen Zwischenbericht erst dann Verfassen, wenn eine Lösung für das fertigstellen der restlichen Meilensteine gefunden wurde und ich kann mit guten Gewissen sage, dass dies sichergestellt wurde und dass Projekt innerhalb der kommenden Wochen fertiggestellt wird.

2 Status

2.1 Meilenstein 1 – Erhebung des Forschungsstandes

Kurzbeschreibung der Haupttätigkeiten

¹ https://openai.com/blog/api-no-waitlist/

² https://github.com/EleutherAI/gpt-neox

³ https://huggingface.co/bigscience/bloom



Erkenntnisse zur Vorgangsweise Kurzbeschreibung der erreichten Ergebnisse Besondere Erfolge/ Probleme Gab es große Abweichungen zum Plan? Warum?

Umfangreiche Literaturrecherche zur Erhebung des Forschungsstandes und der Einordnung der Forschungsarbeit im Vergleich zum erhobenen Forschungstandes.

Dabei wurde zunächst der Fokus auf die einflussreichsten Arbeiten im Bereich der Computerlinguistik und künstliche neuronale Netzwerke gelegt und danach wurden Arbeiten erhoben, die den Teilgebieten des Forschungsprojekts entsprachen.

Es wird aufgezeigt, dass beträchtliche Fortschritte besonders in den letzten 4 Jahren im Bereich der Leistungsfähigkeit von AI basierten Sprachmodellen erfolgt sind. Dieselbe Entwicklungstendenz ist auch im Bereich Bildgenerierung durch Textbeschreibung mithilfe von künstlich neuronalen Netzwerken sichtbar.

Während der Ausarbeitung dieses Meilensteins kam es zu keinen unerwartenden Verzögerungen.

2.2 Meilenstein 2 – Fertigstellung der theoretischen Kapitel

Kurzbeschreibung der Haupttätigkeiten Erkenntnisse zur Vorgangsweise Kurzbeschreibung der erreichten Ergebnisse Besondere Erfolge/ Probleme Gab es große Abweichungen zum Plan? Warum?

Meilenstein 2 beinhalteten Großteiles die Verschriftlichung der erarbeitenden Erkenntnisse aus Meilenstein 1. Zusätzlich wurden bestimmte Keywords erhoben, die der Recherche nach definitiv innerhalb der synthetisch generierten Website vermieden werden müssen, um keine Blockierung des Servers durch den Zensor, strikt basierend auf den Inhalt, zu verursachen. Schlussendlich wurden auch verschiedenste Open Source Tools darauf evaluiert, ob Ansätze verwendet werden, die hilfreich für die Entwicklung des Frameworks sein könnten.

Die Ergebnisse des Meilensteins ist die fertige Verschriftlichung der theoretischen Kapitel, die Fertigstellung der zu vermeidenden inhaltlichen Keywords, sowie die Evaluierung möglicher Open Source Tools die in das Framework eingebunden werden könnten.

Dieser Meilenstein verursachte keine Abweichung des Projektplans.



3 Zusammenfassung Planaktualisierung

Alle Anpassungen des Planungsdokuments kurz zusammengefasst

Aufgrund der erwähnten Verzögerungen wurden die Arbeitspakete für die finalen Meilensteine 4 und 5 verschoben.