A Review on the ChatGPT

Chat GPT & DaKES

【Abstract】This paper presents an concise review of the history and development of ChatGPT, a state-of-the-art language model developed by OpenAI. We explore its origins, technical advancements, impact on society, and future prospects. Furthermore, we discuss the ethical considerations surrounding AI-driven language models and the role of OpenAI in addressing these concerns. By examining the milestones in the development of ChatGPT, we provide insights into the trajectory of natural language processing and AI research as a whole.

1. Introduction

Language models have evolved rapidly over the past decade, transforming our ability to process, understand, and generate human language. Among the most significant developments in this field is ChatGPT, a series of cutting-edge language models developed by OpenAI (Radford et al., 2021). This paper delves into the history and development of ChatGPT, highlighting its milestones, breakthroughs, and impacts on various industries. We also discuss the ethical implications and the ongoing efforts to address them.

2. History and Development of ChatGPT

2.1 GPT-1 and GPT-2

The foundations of ChatGPT can be traced back to the first iteration of the Generative Pre-trained Transformer (GPT) model (Radford et al., 2018). This was followed by GPT-2, which introduced significant improvements in language modeling, generating high-quality text in diverse domains (Radford et al., 2019). Despite these successes, GPT-2's limitations, such as generating plausible but incorrect information and a lack of controllability, prompted the need for further advancements (Brown et al., 2020).

2.2 GPT-3: A Transformative Leap

GPT-3 marked a transformative leap in AI-driven language models (Brown et al., 2020). With 175 billion parameters, GPT-3 achieved unprecedented performance on various natural language understanding (NLU) and natural language generation (NLG) tasks, even surpassing human performance in some instances (Brown et al., 2020; Wang et al., 2020). GPT-3 was also capable of performing zero-shot or few-shot learning, allowing it to adapt to new tasks without retraining (Brown et al., 2020).

2.3 GPT-4: The Emergence of ChatGPT

Building on the success of GPT-3, OpenAI introduced GPT-4, which became the foundation for ChatGPT. With even greater scale and architectural refinements, GPT-4 further improved upon the performance of its predecessors. It enabled more accurate and nuanced language understanding and generation, thus broadening the range of potential applications.

3. Impact on Industry and Society

3.1 Business Applications

ChatGPT's influence spans various industries, including customer service, marketing, content creation, and more. The model's ability to generate coherent and contextually relevant text has led to its widespread adoption in customer support automation, chatbot development, and email drafting, among other tasks (Schwartz et al., 2021).

3.2. Education and Research

The adoption of ChatGPT in educational settings has enhanced learning experiences and research capabilities. Students and educators benefit from its ability to provide instant feedback, generate summaries, and answer questions, while researchers utilize it for literature reviews, data analysis, and hypothesis generation (Gururangan et al., 2020).

3.3. Creative Industries

The creative industries have also harnessed ChatGPT's capabilities. Authors and screenwriters use it to generate story ideas, dialogue, and even entire novels (Zellers et al., 2019). In addition, ChatGPT has found a place in game development as a tool for creating interactive narratives and character dialogues, enriching the overall gaming experience (Riedl & Harrison, 2020).

3.4. Societal Implications

As with any powerful technology, ChatGPT has societal implications. While it has the potential to democratize access to information and accelerate innovation, it also raises concerns regarding disinformation, malicious use, and employment displacement (Brundage et al., 2020). OpenAI acknowledges these concerns and actively works to address them through safety measures, collaboration with external organizations, and user feedback (Radford et al., 2021).

4. Ethical Considerations and OpenAI's Approach

4.1 Addressing Bias

Bias in AI models is a critical concern, as it may perpetuate harmful stereotypes or exhibit unfair behavior. OpenAI has made efforts to reduce bias in ChatGPT by investing in research and engineering to identify and mitigate its sources (Bender et al., 2021). This includes improvements in the fine-tuning process and ongoing engagement with the user community for feedback (Radford et al., 2021).

4.2 Content Filtering and Controllability

OpenAI has implemented content filtering mechanisms to prevent the generation of harmful or inappropriate content. However, these systems are imperfect, and false positives or negatives may occur. OpenAI is committed to refining these mechanisms and making the technology customizable to accommodate user needs and values (Radford et al., 2021).

4.3 Public Input and Collaborative Development

Recognizing the importance of collective decision-making in shaping AI systems,

OpenAI has initiated efforts to solicit public input on system behavior, disclosure mechanisms, and deployment policies. OpenAI also collaborates with external organizations to conduct third-party audits of its safety and policy efforts (Radford et al., 2021).

5. Future Prospects

As ChatGPT continues to evolve, its potential applications will only broaden. Possible future developments include integration with other AI technologies, further improvements in language understanding, and increased capabilities for real-time, interactive communication. The ongoing challenge for researchers and developers lies in balancing the benefits of ChatGPT with the need for ethical and responsible AI deployment.

6. Concluding Remarks

In this paper, we provided a comprehensive review of ChatGPT's history and development, highlighting its milestones, breakthroughs, and impact on various industries. The advancements in natural language processing and AI research have been remarkable, and ChatGPT serves as an excellent example of the capabilities of these technologies. While the ethical considerations surrounding AI-driven language models warrant careful attention, OpenAI's commitment to addressing these concerns sets a positive precedent for future developments. As we continue to explore the potential of ChatGPT and other AI systems, it is essential to balance their benefits with responsible and ethical deployment.

References

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?. Proceedings of the 2021 ACM FAccT.

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., ... & Amodei, D. (2020). Language Models are Few-Shot Learners. Advances in Neural Information Processing Systems, 33.

Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., ... & Maharaj, T. (2020). Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims. arXiv preprint arXiv:2004.07213.

Gururangan, S., Marasović, A., Swayamdipta, S., Lo, K., Beltagy, I., Downey, D., & Smith, N. A. (2020). Don't Stop Pretraining: Adapt Language Models to Domains and Tasks. Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics.

Radford, A., Narasimhan, K., Salimans, T., & Sutskever, I. (2018). Improving Language Understanding by Generative Pre-Training. OpenAI Blog.

Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). Language Models are Unsupervised Multitask Learners. OpenAI Blog.

Radford, A., Gokaslan, A., Mann, B., Sutskever, I., Rosanne, L., & Amodei, D. (2021). ChatGPT: Lessons from Scaling AI. OpenAI Blog.

Riedl, M. O., & Harrison, B. (2020). Using AI to Generate NPCs and Quests for Video Games. Communications of the ACM, 63(11), 60-61.

Schwartz, R., Dodge, J., Smith, N. A., Etzioni, O., & Hajishirzi, H. (2021). Green AI: Building

Efficient AI Applications. Communications of the ACM, 64(1), 54-63.
Wang, A., Singh, A., Michael, J., Hill, F., Levy, O., & Bowman, S. R. (2020). GLUE: A Multi-Task Benchmark and Analysis Platform for Natural Language Understanding. In Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing (EMNLP).
Zellers, R., Holtzman, A., Rashkin, H., Bisk, Y., Farhadi, A., Roesner, F., & Choi, Y. (2019). Defending Against Neural Fake News. Advances in Neural Information Processing Systems, 32.

ChatGPT发展综述

Chat GPT & DaKES

【摘要】本文简要回顾了 ChatGPT 的历史和发展，ChatGPT 是 OpenAI 开发的一种最先进的语言模型。 我们探索它的起源、技术进步、对社会影响以及未来前景。 此外，我们讨论了围绕 AI 驱动的语言模型的伦理考虑以及 OpenAI 在解决这些问题中的作用。 通过检查 ChatGPT 发展的里程碑，我们提供了对自然语言处理和 AI 研究整体轨迹的见解。【中文版非英文版完全对应】

1. 引言

语言模型在过去十年中发展迅速，改变了我们处理、理解和生成人类语言的能力。 该领域最重要的发展之一是 ChatGPT，这是由 OpenAI 开发的一系列尖端语言模型（Radford 等人，2021）。 本文深入探讨了 ChatGPT 的历史和发展，重点介绍了它的里程碑、突破和对各个行业的影响。 我们还讨论了道德影响以及解决这些问题的持续努力。

2. GPT-1 和 GPT-2

ChatGPT 的基础可以追溯到生成预训练转换器 (GPT) 模型的第一次迭代（Radford 等人，2018 年）。 随后是 GPT-2，它在语言建模方面进行了重大改进，在不同领域生成了高质量的文本（Radford 等人，2019 年）。 尽管取得了这些成功，但 GPT-2 的局限性（例如生成看似合理但不正确的信息以及缺乏可控性）促使需要进一步改进（Brown 等人，2020 年）。

3. GPT-3：变革性的飞跃

GPT-3 标志着 AI 驱动的语言模型的变革性飞跃（Brown 等人，2020 年）。GPT-3 拥有 1750 亿个参数，在各种自然语言理解 (NLU) 和自然语言生成 (NLG) 任务上取得了前所未有的性能，甚至在某些情况下超过了人类的性能（Brown 等人，2020 年；Wang 等人，2020 年） . GPT-3 还能够执行零样本或少样本学习，使其无需重新训练即可适应新任务（Brown 等人，2020 年）。

从 ChatGPT 时代往回看，也许 OpenAI 在 GPT-2 中的发现确实坚定了他们对 GPT 系列模型的信心，并决定加大研发投入力度。因为在随后的 2020 年他们发布了 1750 亿参数量的 GPT-3，一个即便以现在的眼光去看也大得让人惊叹的模型。虽然 OpenAI 没有明确公开训练这个模型的费用，但大家的估算是当时花了 1200 万美元。同时公开的还有一篇长达 60 多页的论文（Language Models are Few-Shot Learners），其中详细阐述了这个新的庞然巨物所展示出来的新能力。最重要的发现莫过于论文标题中所说的，语言模型具有小样本（few-shot）学习的能力。

小样本学习是一个机器学习领域的专业术语，但它有着很朴素的理念，即「人类是可以通过少量的几个例子就学会一个新的语言任务」。想象一下在语文课上学习怎么掌握「把」字句换成「被」字句样（雨把衣服淋湿了 —— 衣服被雨淋湿

了）的情形，老师会给出几个例子，同学们就能够掌握这项能力。

但对于深度学习模型来说，它通常需要学习（训练）成千上万的例子才能掌握一项新的能力，但大家发现 GPT-3 却像人类一样具有类似的能力。而且重点在于，只需要给它展示几个例子，它就会「有样学样」地完成例子给出的任务，而不需要进行额外的训练（即不需要进行常规训练中的梯度反传和参数更新）。后来的研究表明，这种能力是巨型模型所特有的，被业内叫做「在上下文中学习」（in context learning）的能力。

实际上，小样本学习能力本身并不是很惊人的发现。毕竟业内一直都在对小样本学习进行研究，很多专攻小样本学习的模型都有出色的小样本学习能力。但 GPT-3 展示出来的这种「在上下文中学习」的小样本能力却非常出人意料，其原因也和 GPT-2 所展示的多任务能力一样

GPT-3 并没有为了获得小样本的能力而在训练数据、训练方式上做特别的设计，它依然只是一个用语言模型任务训练的生成式模型；GPT-3 的小样本能力是以「在上下文中学习」的方式展现出来的。换句话说，想让它获得新的能力，不需要对它再训练，而只需要给它看几个示范的例子。

除了这个能力以外，GPT-3 还展示出了优秀的文本生成能力，相比 GPT-2，它生成的内容更加流畅，而且可以生成很长的内容。这些能力综合体现在一个模型上，让 GPT-3 在当时成为了大家的关注焦点，它也成为 OpenAI 正式对外提供服务的模型。

但随着这个模型服务的开放，越来越多的人尝试使用这个模型。从这时起，OpenAI 通过开放给公众的方式，同时也在收集着更具有多样性的数据（用户使用时输入的内容可能会被用于模型的训练，这一点是写在用户条款中的），这些数据在后来的模型迭代中也发挥着重要的作用。自此 GPT 系列模型的数据飞轮便转动了起来，越多优质的用户数据，迭代出效果越好的模型。

与 ChatGPT 不同的是，GTP-3 并不是采用对话的形式交互的模型，而是一个文本的续写模型（也就是在你输入的文字后面接着往下写），因此它并不具备如今的 ChatGPT 所拥有的多轮对话能力。但它已经能够干很多的事情，例如编写故事、给邮件做自动补全等等。但同时，大家也慢慢发现了一些问题，例如它会一本正经地输出不符合事实的内容，并且会输出一些有害的言论等等。这是这种文本生成模型最突出的弊端，虽然经过多次迭代，但 ChatGPT 如今也依然面临类似的问题。

4. CodeX：让计算机自己写代码

OpenAI 在对 GPT-3 的研究中还有一个意外的发现，它能够根据一些注释生成很简单的代码。因此在随后的 2021 年，他们对生成代码这件事情进行了专门的研究投入，并发布了 CodeX 模型。它可以看作是一个有着代码专精能力的 GPT 模型，能够根据自然语言输入生成比较复杂的代码。

从外部视角来看，我们无法判断代码生成的研究与 GPT 系列模型的研发是否在同时进行。但放在当时，让模型具有生成代码的能力，从实用化的角度来说确实更加具有意义，毕竟 GPT-3 还未拥有如今 ChatGPT 这般强悍的能力。另一方面，让模型去生成代码也能规避它生成有危害文本内容带来的风险。

在 CodeX 论文中提及了几个要点，首先是让经过文本数据预训练的 GPT 模型在专门的代码数据（数据来自 github 的开源代码，一共 159G）上训练确实能够明显提升模型对代码的理解和输出能力。其次是论文中用的是一个 120 亿参数的「小」模型，这个信息从侧面反映出 OpenAI 内部除了对外开放接口的 1750 亿参数的 GPT-3 模型外，还有别的不同大小的模型版本。

而加入代码训练，让模型获得理解和生成代码的决定，原本的初衷也许只是希望 GPT 能够多一种应用场景。它看似与 GPT 系列模型在理解和运用自然语言的能力没有太大的联系，但根据后续的研究（详细的分析请参考文章《拆解追溯 GPT-3.5 各项能力的起源》），增加对代码数据的训练很有可能触发了后来的 GPT 模型在自然语言上的复杂推理和思维链的能力。

也许在 OpenAI 做 CodeX 之初并没有预料到会有这样的结果，但就像他们一直使用文本生成任务来做 GPT 模型，然后在 GPT-2 和 GPT-3 中「解锁」了「多任务的能力」和「在上下文中学习的能力」那样，代码数据的引入又一次让他们获得了意料之外的收获。虽然看上去似乎有一些偶然，但对技术路线的前瞻性认知，加上坚持与持续的投入显然是一个至关重要的因素。

5. InstructGPT：让 GPT 好好说话

在前面我们提到了 GPT-3 虽然已经有很强的能力，但上线以后随着使用的人越来越多，也发现了很多问题，最严重的应该要数「一本正经地胡说八道」和「输出带有危害性的内容」这两点了。虽然在 2021 年 OpenAI 似乎暂时将重点放在了让模型理解和生成代码这件事情上，但他们应该一直在尝试解决 GPT-3 的这些问题。

在 2022 年初，OpenAI 发表了 InstructGPT 的论文（Training language models to follow instructions with human feedback），从中我们可以一窥解决这些问题的方法。论文的核心理念是让模型接受人类的教导（反馈），这一点在标题中就已经开宗明义了。

GPT-3 之所以会出现「一本正经地胡说八道」和「输出有害的内容」这样的问题，其根源来自于它所使用的训练数据。像 GPT-3 这样的庞然大物，对数据的需求量是海量的。我们从 GPT-3 的论文中可以找到它的数据来源，大致可以划分为三类：网页内容、百科内容以及书籍。虽然网页内容的量非常大，但也非常「脏、乱、差」，自然会包含很多非真实性和有害的内容。GPT-3 在这些数据上进行训练，自然也就学到了这些东西。

但作为一款对外提供服务的产品，GPT-3 的回答应该更小心一些。要解决这个问题，其中的一难点在于怎么去定义模型应该怎么说话。因为生成模型的输出内容是自然语言本身，而不是一个分类的标签或一个实体名词这种有明确的、客观对错的内容。没有明确的对错，就导致无法像训练经典的 NLP 模型那样直接针对目标设计训练任务。

而 InstructGPT 给出的解决思路是非常直接的，既然对于「好的回答」这个评价指标有很多不同的影响因素，这些因素又相互交织在一起，那就让人来教它怎么写回答。因为人类是比较善于处理这种「既有明确的要求，又有模糊的范围」的问题的，让真人写一些「优秀范例」，让模型去学习这些「优秀范例」，这正是

InstructGPT 提出的总体思路。

具体而言，InstructGPT 提出了两个阶段的路径来让 GPT 学习人类给出的「优秀范例」，第一阶段是监督学习，第二阶段是强化学习。在第一阶段中（对应下图中最左边的 Step 1），让真人根据不同的 Prompt（粗浅可以认为是我们使用 ChatGPT 时，在对话框里输入的那条文本，在业界这个东西叫做指令）写真实的、无害的、有用的回答。实际操作过程中，为了保证这些内容的质量，会给写回答的标注人员一些规范性的指引，然后让已经经过预训练的 GPT 模型在这些人类编辑的数据上继续训练。这一阶段可以看作是对模型的一种「规训」，用一个不严谨的类比来说，就像语文老师让你默写优秀范文那样。

第二阶段是强化学习，技术上分为两步。第一步（对应上图中间的 Step 2）是让被「规训」后的模型根据不同的 Prompt 生成多个不同的回答，并由人来给这些回答按照好与差的标准来排序。然后用这些标注了优劣之分的数据训练一个打分模型，让它可以自动给更多的数据进行排序打分。强化学习阶段的第二步（对应上图中右边的 Step 3）就是利用这个打分模型作为强化学习中的环境反馈，以策略梯度（Policy Gradient，准确地说是 PPO 算法）的方式对已经「规训」后的 GPT 模型进行训练。整个第二阶段的过程可以看作是对模型的一种「强化」，再用一个不严谨的类比来说，就像语文老师给你写的作文打分，让你从分数中分辨什么是好与不好，然后不断进步。

因此，用一种非常不严谨，但普通人或许也能够理解的方式来说，InstructGPT 先是让一个「口无遮拦」的 GPT 通过「默写人类的优秀范文」的方式初步学会「好好说话」，然后再「给它独自写出来的东西打个分，让它回去好好领悟，继续进步」。当然，在技术上牵涉事情会更复杂一些，比如「优秀范文」的具体规范和数量等数据上的问题，以及强化学习中打分模型的选择，算法参数的设置等算法上的问题，都会对最后的效果产生影响。但最终的结果表明，这种方式是非常有效的，论文中也指出一个通过上述方式训练出来的 13 亿的小模型，效果就能够超过没有经过这种训练的更大的模型。

另外论文中还有一些非常值得一提的内容。首先是关于 Prompt 的一些发现。InstructGPT 训练时所使用的 Prompt 主要由两部分构成，一部分是专门的 AI 训练师编写的，另一部分自来 OpenAI 的模型在线服务期间，由用户使用中编写的内容，这时数据飞轮的作用就体现了。可以发现，无论是哪种，这些 Prompt 都是由真人写出来的，虽然文章中没有对这些 Prompt 的具体涵盖范围、分布情况以及提问的方式展开详细的分析，但可以合理地猜测这些 Prompt 具有一定的多样性和较高的质量。其实文章中对比了使用这些真人编写的 Prompt 训练的模型和使用一些开源 NLP 任务数据集中构建的 Prompt（例如 T0 数据集、FLAN 数据集）训练出来的模型，结论是由真人编写 Prompt 训练出来的模型，给出的答案更加能被评测的人接受。

另外一点是关于训练好的模型对新的 Prompt 的泛化能力的问题，可想而知的是，如果训练完成的模型无法产生 Prompt 的泛化能力，那么现在 ChatGPT 所表现出来的，几乎百问百答的能力是不太可能产生的。因为在模型做微调的阶段，即便是再多的数据，也不可能把人们有可能会输入的内容都覆盖完整。而 InstrctGPT 论文中点明了文中所采用的方法是可以产生 Prompt 的泛化能力的。

6. GPT-3.5 时代和 ChatGPT 的诞生

在随后的时间内，OpenAI 发布了多个被称为 GPT-3.5 系列的模型，虽然这些模型并未有相关的论文跟随发表，但根据这篇文章的分析，GPT-3.5 系列应该是融合了 OpenAI 在 GPT-3 时代积累的技术、数据以及经验开发出来的。由于没有详细的官方公开信息参考，关于这些模型的具体资料，外界主要是通过分析使用的体验、相关的技术论文以及 OpenAI 的 API 文档介绍来进行推测。

根据分析，GPT-3.5 系列的模型有可能并不是在 GPT-3 上继续微调而来，而很可能是将代码和自然语言的数据融合在一起，重新从零开始训练了一个基础模型。这个模型可能比 GPT-3 的 1750 亿参数量更大，它在 OpenAI 的 API 中被命名为 codex-davinci-002。然后在这个基础模型上，通过指令微调和人类反馈得到了一系列后续的模型，包括 ChatGPT。

简要地说，从 code-davince-002 这个模型开始，经过有监督的指令微调得到 text-davinci-002。以及后续的 text-davinci-003 和 ChatGPT，也是在 GPT-3.5 系列的某个模型上通过指令微调以及人类强化学习反馈得到的。并且 text-davinci-003 和 ChatGPT 都是在 2022 年 11 月发布的，不同的是 text-davinci-003 和 GPT-3 一样，是一个文本补全模型。而根据 ChatGPT 的官方介绍，它是通过将过往的数据处理成对话交互的形式，并增加了新的对话数据训练出来的。

至此，我们大致回顾了 OpenAI GPT 系列模型从 2018 年的初代 GPT 到现在的 ChatGPT，一路发展迭代的过程。在这个过程中，OpenAI 一直保持着对生成式预训练模型这一技术路径的「执拗」，并且也一直从不断发展的 NLP 技术中吸纳新的方法，从最初的 Transformer 模型结构，到后来的指令微调（Prompt tuning）等技术的出现，这些因素共同促成了如今 ChatGPT 的成功。

7. ChatGPT的成功

ChatGPT 所带来的惊艳效果是由许多不同的 NLP 任务综合体现出来的，但在分析它背后的技术时，还是通过将它的能力进行拆解会更加清晰明了一些。总体而言，ChatGPT 所体现出来的能力可以大致划分为以下几个维度：

- 文本生成的能力：ChatGPT 的所有输出都是即使生成出来的文本，所以文本生成的能力是它最基本的要求。

这一项能力实际上是来自于它的训练方式，ChatGPT 在预训练时，是一个标准的自回归语言模型任务，这是 OpenAI 所有 GPT 系列模型的基底。所谓的自回归语言模型任务，通俗的理解是这样的：它可以根据已经输入的文本，预测下一个 token 应该是什么。这里所说的 token，所代表的是模型所使用的最小单位的字符片段，它可以是字（在中文里采用字是很常见的），也可以是词（英文的每个词天然地被空格隔开了，所以常采用词），甚至是字母。但现在的方法通常采用的是子词（subword，介于字母和词之间，主要的目的是减少词表数量）。但不论是哪种，自回归语言模型任务的基本思路都是根据已经输入的文本，预测下一个要输出的文本是什么，就像下图的例子中那样

在训练的时候，会准备很多文本数据，比如网页上的文章、各类书籍等等，只要是正常的文字内容，都可以用来训练。值得说明的是，这种数据不需要进行额外

的人工标注，因为这类数据本来就是人写的，模型要做的事情就是根据这些人写出的文本，去学习「给定了前面的文字，接着这些文字后面这个地方应该是什么」的问题。这便是业内所称的「无监督训练」，实际上模型并不是真的没有监督（不然模型学什么呢？），只是它的数据不需要额外的人工标注。也正因为这个任务是不需要额外标注的，因此可以「免费」获得大量的数据，得益于互联网的普及，可以「轻松地」获得海量的由真人写出的文本内容用来训练。这一点也是 GPT 系列模型的特点之一，用海量的数据，去训练很大的模型。

- 丰富的知识储备：ChatGPT 能够正确回答非常多的问题，包括历史、文学、数学、物理、编程等等。因为目前版本的 ChatGPT 并没有利用外部知识，因此这些知识的内容是「储存」在模型内部的。

ChatGPT 所拥有的丰富知识储备，来自于它的训练数据，以及它足够大的体量，以便学会这些内容。虽然官方并没有公开 ChatGPT 所使用的训练数据的具体细节，但从它的前身 GPT-3 的论文可以推测，这些数据大致可以分为三个大的范畴：网页内容、书籍内容以及百科内容。可想而知的是，这些内容天然地蕴含了大量的知识，百科和书籍自然不必说，而网页内容也包含了许多新闻、评论、观点等，并且网页也包括了很多专门的问答垂直类网站，这些都是 ChatGPT 的知识来源。在官方的介绍里指出 ChatGPT 无法回答 2021 年以后发生的事情，因此合理的猜测是训练的数据收集截止到 2021 年。

但数据量只是其中一个方面，要让模型「掌握」这些数据，其自身的体量是不可能小的。以 GPT-3 为例，它有 1750 亿参数，可以粗浅地理解为，这些数据的内容以及模型的各项能力，都以这一个个参数的具体数值的形式，固定在了训练完成的模型中。感性的理解是，假设一个模型只有 1 个参数，那它什么也干不了。更严谨的分析和对比可以参考这篇论文《Holistic Evaluation of Language Models》的测评，方向性的结论是越大的模型，在需要知识来完成的任务上表现得越好。

论文地址：https://arxiv.org/pdf/2211.09110.pdf

- 逻辑推理与思维链的能力：从第一章图片中的鸡兔同笼的例子可以看出，ChatGPT 具有很强的逻辑推理能力。并且它能够将复杂的内容，通过拆解，分成多个小的步骤，一步步地进行推理，获得最后的答案，这种能力被称为思维链。

但如果没在代码上做过训练的话，只有很弱或几乎没有思维链和推理能力。而 ChatGPT 确实是在代码数据上进行过训练的，这一点从它能够理解并生成代码也可以看出来。在第二章回顾发展历程中提到了，OpenAI 在 2021 年就发布了专门针对代码的 CodeX 模型，将代码数据加入 GPT 的训练数据应该就是从那时开始的。

- 按照人的提问或者指令给予回复的能力：ChatGPT 除了可以用狭义的基于「问答」形式的交互以外，还能够按照输入的要求进行回复。例如，在应对「帮我写一封信」这类指令式的要求时，它同样也展现出了优秀的能力。这种能力让它不仅是一个提供答案的「高级搜索引擎」，更是一种可以用自然语言来交互的文字处理工具。

虽然目前大众普遍把目光聚焦在将 ChatGPT 作为一种类搜索引擎的工具，但查阅相关知识并给予回答并不是它的唯一能力。实际上，单就 ChatGPT 本身而言，回答知识性的问题并不是它的强项，毕竟它本身的训练数据被定格在了 2021

年。即便用更新的数据去训练，但它终究跟不上时事的变化，因此要将它用作知识性的问答工具，还是需要与搜索引擎等外部知识源做结合，就像现在 Bing 做的一样。

ChatGPT 根据输入的指令（prompt）进行回复的能力，是来自于一种被称为指令微调的模型训练方式（prompt tuning）。其实原理很简单，模型依然还是「根据输入的内容，预测下一个 token 是什么」，只是在指令微调的阶段，输入的内容被换成了这些事先写好的 prompt，而 prompt 后面需要生成的内容，则是事先写好的答案。因此在这一阶段和一开始所说的无监督自回归语言模型训练，最大的不同在于数据。这里的数据，也就是 prompt 以及对应的回复，都是人写的，换句话说，这一阶段用的是人工标注的数据进行的监督训练。

提到人工标注的数据，就自然牵涉到了所需要的数据量了，因为每一条标注数据都是需要成本的。如果是不需要标注（就像第一阶段的训练），那么自然有海量的文本数据可供训练，但如果要标注，那到底需要多少这种数据呢？要知道，让标注人员手写一个 prompt，然后再手写一个几百字的、真实详尽的回答，成本是很高的。根据论文《Training language models to follow instructions with human feedback》的介绍，所需要的数据其实不需要太多（相比于无监督阶段所使用的数据来说）。虽然具体到 ChatGPT 到底使用了多少没有确切的信息公开，但可以确定的是在数量级上一定远比用来进行无监督训练的网页、百科和书籍所构成的数据集要小非常多。

论文地址：https://arxiv.org/pdf/2203.02155.pdf

只需要相对少量的人工标注的 prompt 数据就能达到让模型按照指令做出回复的目的，这一点背后其实隐含了一个现象，在学界内被称为 prompt 的泛化能力。可以想象一下，如今全世界都在不停的向 ChatGPT 提问，所提的问题也必定是千奇百怪的，这些问题其实就是一个个的 prompt。但用来对 ChatGPT 进行指令微调的 prompt 肯定不会有这么多，这说明模型在学习到了一定量的 prompt 和相应的答案以后，它能够「举一反三」地对它没有见过的 prompt 进行回答，这就是 prompt 的泛化能力。文章《拆解追溯 GPT-3.5 各项能力的起源》分析指出，这种泛化能力与在指令微调阶段让模型学习的标注数据数量以及多样性相关。

此外，用少量的 prompt 数据就能微调出类似于 ChatGPT 这样拥有强大能力的模型，背后还隐含了另一个猜测，即模型所表现出来的各项能力，可能在无监督训练的阶段就已经存在于模型当中了。其实这也很好理解，毕竟相比于无监督的数据，这些人工标注的 prompt 数量太少了，很难想象模型是通过对这些仅有的标注数据学习而产生了各种各样的能力。从这个角度来说，指令微调的过程更多只是让模型学会按一定的规范来进行回复，而它的知识、逻辑等能力是早已存在的。

- 「客观公正」的能力：如果对 ChatGPT 询问一些有害或者有争议的问题，可以看到 ChatGPT 的回答都是非常「小心」的，很像是经过训练的新闻发言人般的回答。虽然它目前依然做得不够好，但这种能力是 OpenAI 敢将它公开作为一款产品使用的核心因素。

让模型的输出符合人类的价值观是 OpenAI 一直在做的事情。早在 2020 年 GPT-3 的时候，OpenAI 就发现这种通过网上的数据训练出来的模型，会生成带有歧视、危险、争议的内容。作为一个对外提供服务的产品，这些有害的内容显然是

不合适的。而现在的 ChatGPT 在这一点上有着明显的改善，让模型做出这种「行为改变」的主要方法也来自于 InstructGPT 的论文，更确切地说，是通过有监督的指令微调加上人类反馈的强化学习共同完成的。

从技术方法的角度来说，ChatGPT 相关的内容都是已知的，但为什么当前只有它拥有如此惊艳的表现呢。实际上从 ChatGPT 推出之后，NLP 社区就一直在分析这其中的原因，主要有：

模型体量的因素

能力涌现出现的前提是模型体量达到一定的规模，虽然没有具体的指标指引，但从目前的事实情况来看，类似于思维链等比较「高级」的能力，需要在数百亿参数量以上的模型中才表现得足够优异。

数据量的因素

模型的大小不是唯一的因素。DeepMind 在这篇论文《Training Compute-Optimal Large Language Models》提供了一些分析性的结论，指出训练的数据量需要随着模型的体量相应地增加，更确切地说，是模型训练时「见过的 token」数量，需要随着模型体量增加。

论文地址：https://arxiv.org/pdf/2203.15556.pdf

数据质量的因素

对于无监督的数据，数据量相对而言并不是很大的障碍，但数据质量往往更加容易被忽视。实际上在 GPT-3 的论文中，就有专门的内容介绍数据的处理工作。为了清洗 GPT-3 的训练数据，OpenAI 专门训练了一个数据过滤模型，来从海量的网页数据中获取更高质量的数据。相比而言，与 GPT-3 体量相当的一些开源模型，例如 Meta 的 Opt 和 BigScience 的 Bloom，似乎没有进行这一步清洗。这也许是这两个开源模型效果劣于 GPT-3 的原因之一。

此外，数据质量的衡量维度不是单一的，诸如数据的多样性、内容重复度以及数据的分布情况都是需要考虑的因素。例如虽然 GPT-3 所使用的网页、百科、书籍这三大类数据中，网页数据的总量是最多的，但在训练时这三类数据的采样并不是按照实际数据的多寡进行的。

另外值得一提的是，在指令微调的阶段，采用人工编写指令也许是一个重要的影响因素。InstructGPT 的论文明确指出在测评过程中，采用人工编写的指令训练出来的模型，比采用现有的 NLP 数据集通过模版的方式构建指令训练出来的模型有更好的效果。这也许解释了在 T0、FLAN 等由 NLP 数据集构成的指令数据集训练出来的模型为什么效果会差一些。

训练过程的影响

这类巨型模型在训练时通过集群进行训练，同时采用数据并行、模型并行以及 ZeRO 优化器（一种降低训练过程显存占用的方法），这些方式为训练的稳定性引入了更多的变量。如下这篇分析指出甚至模型是否采用 bfloat16 精度都对结果有明显的影响。

分析链接：https://jingfengyang.github.io/gpt

相信了解了上面的这些内容，大家对复刻一个类 ChatGPT 的方式以及会面临的问题会有一个大致的了解。有幸的是 OpenAI 已经证明了这技术路径是能够走通的，ChatGPT 的出现也确实正在改变 NLP 技术的发展走向。

8. GPT-4：ChatGPT Plus

基于 GPT-3.5 的成功，OpenAI 推出了 GPT-4，它成为 ChatGPT Plus的基础。 随着更大的规模和架构的改进，GPT-4 进一步改进了其前身的性能。 它使更准确、更细微的语言理解和生成成为可能，从而扩大了潜在应用的范围。

这种生成式模型搭配 prompt 的方式，直接略过了中间的各项 NLP 能力组件，用最直接的方式解决应用场景的问题。在这种范式下，完成终端应用的技术路径将不再是用单点 NLP 能力模块通过搭积木的方式组合起来。

ChatGPT 可看作是一个以自然语言作为交互媒介的 NLP 工具。如果说过去我们是通过模型 + 数据 + 设计训练任务的方式来完成某项 NLP 能力，那么 ChatGPT 则是通过设计指令来完成这些能力。

接下来的事情就震惊世界了：

2023年3月14日，GPT-4发布，OpenAI给出了技术报告和3分钟的预告片。GPT-4支持多模态，能够识图、生成歌词、做网站，并且刷爆了人类社会各个领域的考试，已经达到了哈佛、斯坦福等顶尖高校的水平。现已集成到微软New Bing和ChatGPT Plus。

3月16日，OpenAI 的首席科学家兼联合创始人Ilya Sutskever表示OpenAI不会分享更多关于GPT-4的信息。Sutskever表示出于竞争和安全的考量，当然主要是同行的竞争，当被问及为什么 OpenAI 改变了分享其研究成果的方式时，Sutskever 简单地回答说：坦率地说，我们错了。如果你像我们一样相信，在某个时候，人工智能将变得极其强大，那么开源就没有意义了，我完全希望在几年内，每个人都会完全清楚开源 AI 是不明智的。

3月17日，微软Microsoft 365全面引入生成式AI助手Copilot，将GPT-4集成到了Word、Excel、PowerPoint、Outlook和Teams等应用中，用户可以提出问题并提示AI撰写草稿、制作演示文稿、编辑电子邮件、制作演示文稿、总结会议等。

3月20日，OpenAI发布了GPT模型和技术对劳动力市场潜在影响的论文，预计将影响80%的工作岗位。

已构建好技术壁垒的OpenAI开始拒绝技术开源，甚至DeepMind 首席执行官Demis Hassabis也同样表示：我们正在进入一个时代，我们必须开始考虑贪图便宜的人，或者那些正在阅读但没有为该信息库做出贡献的人，这也包括民族国家，这很明显，你可能会想到谁。他表示人工智能行业公开发布其发现的文化可能很快需要结束。

回归到技术本身，OpenAI表示在发布GPT-4之前，他们花费了八个月进行安全研究、风险评估和迭代，因此，GPT-4的初始可用日期是在2022年8月。GPT-4是包括视觉语言模型组件的大型语言模型，类似于DeepMind的Flamingo模型，输入可以是文本或图像，但所有的输出都是文本。

GPT-4 的数据收集是由 Wojciech Zaremba（数据集团队经理）和 Qiming Yuan（数据集采购和处理负责人）领导的一项艰巨任务。数据集贡献来自一个由 35 名 OpenAI 员工组成的团队。在预训练阶段，OpenAI过滤了 GPT-4 的数据集组合，以专门减少不适当的色情文本内容的数量。通过结合内部训练的分类器和基于词典的方法来识别被标记为极有可能包含不当色情内容的文档。

OpenAI 拥有利用来自包括谷歌在内的竞争对手的其他数据集的经验，依赖最先进的 DeepMind MassiveText 和 Google Infiniset数据集，且OpenAI 与 Microsoft 的合作伙伴关系允许访问 GitHub 等大型数据集，我们可以推测GPT-4可能是在1.7T-2.9T的文本tokens上进行的训练，模型参数量包括800-1400亿的语言模型参数+200亿的视觉模型参数。

此外，GPT-4的文本生成长度被显著提高，一个token通常对应大约 4 个字符，而1个汉字大致是2~2.5个token，在GPT-4之前，token的限制大约在4096左右，大约相当于3072个英文单词，一旦对话的长度超过这个限制，模型就会生成不连贯且无意义的内容，到了GPT-4其最大的token数是32768个，大约相当于24576个单词，相当于48页文本，生成长度被扩大了八倍。

于是，人类迎来AI-GPT大爆发时代。

参考文献

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?. Proceedings of the 2021 ACM FAccT.

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., ... & Amodei, D. (2020). Language Models are Few-Shot Learners. Advances in Neural Information Processing Systems, 33.

Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., ... & Maharaj, T. (2020). Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims. arXiv preprint arXiv:2004.07213.

Gururangan, S., Marasović, A., Swayamdipta, S., Lo, K., Beltagy, I., Downey, D., & Smith, N. A. (2020). Don't Stop Pretraining: Adapt Language Models to Domains and Tasks. Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics.

Radford, A., Narasimhan, K., Salimans, T., & Sutskever, I. (2018). Improving Language Understanding by Generative Pre-Training. OpenAI Blog.

Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). Language Models are Unsupervised Multitask Learners. OpenAI Blog.

Radford, A., Gokaslan, A., Mann, B., Sutskever, I., Rosanne, L., & Amodei, D. (2021). ChatGPT: Lessons from Scaling AI. OpenAI Blog.

Riedl, M. O., & Harrison, B. (2020). Using AI to Generate NPCs and Quests for Video Games. Communications of the ACM, 63(11), 60-61.

Schwartz, R., Dodge, J., Smith, N. A., Etzioni, O., & Hajishirzi, H. (2021). Green AI: Building Efficient AI Applications. Communications of the ACM, 64(1), 54-63.

Wang, A., Singh, A., Michael, J., Hill, F., Levy, O., & Bowman, S. R. (2020). GLUE: A Multi-Task Benchmark and Analysis Platform for Natural Language Understanding. In Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing (EMNLP).

Zellers, R., Holtzman, A., Rashkin, H., Bisk, Y., Farhadi, A., Roesner, F., & Choi, Y. (2019). Defending Against Neural Fake News. Advances in Neural Information Processing Systems, 32.