大数据与决策研究

（政策与技术跟踪专题）

2023 年第 2 期（总第 158 期）

广西壮族自治区信息中心
广西壮族自治区大数据研究院　　2023 年 2 月 16 日

编者按：ChatGPT 是由 OpenAI 公司推出的一款人工智能聊天机器人程序，能实现撰写邮件、视频脚本、文案、翻译、代码，写论文等任务，被认为正在“掀起新一轮 AI 革命”。ChatGPT 上线不到一周日活用户破百万，2 个月破亿，迅速火爆全网，成为史上用户增长速度最快的消费级应用。ChatGPT 的推出将不断拓展海量应用场景，赋能传统领域智能化发展，推动 AI 行业开启新发展浪潮。

本期要目

◆ ChatGPT 的概念特征及发展现状
◆ ChatGPT 的技术发展路径
◆ ChatGPT 的未来应用场景

ChatGPT 的概念特征及发展现状

一、ChatGPT 的概念特征

ChatGPT 是由人工智能研究实验室 OpenAI 在 2022 年 11 月 30 日发布的全新聊天机器人模型，一款人工智能技术驱动的自然语言处理工具。它能够通过学习和理解人类的语言来进行对话，还能根据聊天的上下文进行互动，真正像人类一样来聊天交流，甚至能完成撰写邮件、视频脚本、文案、翻译、代码等任务。

表 1 ChatGPT 特点

特点	功能
对话型模型	工作原理是用户输入文字和话语，模型给一段输出，类似于人的对话模式，与传统 NLP 模型相比有很高的精度。
文生文/文生图	在文字处理上，有文字的生成、扩写或改写功能。人们提供想法、创意或者主题，模型可以生成故事、文章等输出。
具有代码生成能力	除了人类语言的训练之外，还做了代码的训练，把很多开源代码给模型学习。比如给 5 个数字进行排序这样的问题，模型会输出可执行的代码。
弱推理能力	可以回答一些需要推理才能回答的模型，比如给长宽求面积。

资料来源：根据公开信息整理、招商证券

ChatGPT 是在 GPT3.5 大模型语言模型（LLM，即 Large Language Model）的基础上，加入“基于人类反馈的强化学

习（RLHF，Reinforcement Learning from Human Feedback）”来不断微调（Fine-tune）预训练语言模型，使得 LLM 模型学会理解不同类型的命令指令，并通过多重标准合理判断基于给定的 prompt 输入指令，输出的是否为优质信息（这些标准包括：富含信息、内容丰富、对用户有帮助、无害、不包含歧视信息等）。

二、ChatGPT 的优势与独特性

目前，ChatGPT 不需要任何额外的训练就能在多种不同的领域中应用并快速输出高质量的文本，相较于以前的模型已具备较强的自然语言处理能力，具体来讲可归纳为以下几点：

第一、更强的对话能力：ChatGPT 支持多轮对话，在自然语言交互方面、情感分析、情景会话等方面运行流畅，在语言模仿能力和逻辑判断方面展现出更强的能力。

第二、更全面的语言能力：ChatGPT 支持多种语言环境，并且支持长短句输入，在阅读理解、复杂语句处理、逻辑能力和文本生成方面更加灵活。

第三、更高精度的预测结果：ChatGPT 的训练模型支持大规模数据集，具备海量的话题库，通用性更强。

三、ChatGPT 现存的缺陷和发展瓶颈

（一）精准性、真实性、重复率和依赖性尚待改善

第一、由于技术实现的问题，ChatGPT 会不可避免地写出一些似是而非或者荒谬的答案，这将导致植入虚假数据和误导用户的风险。ChatGPT 依然没有完全克服大型语言模型

（LLM）的这一常见缺点，造成这个问题的原因主要有以下三点：（1）在训练和强化学习（RL）的过程中，数据集中没有对应的事实或标准答案的来源；（2）训练模型时谨慎性提高，为了避免误报等情况，可能导致模型拒绝可以正确回答的问题；（3）监督训练中行为克隆（BC，Behavior Cloning）对模型产生误导：当模型掌握的信息量高于训练者（human expert），模型会采集冗余信息；当训练者的常识信息量高于模型，基于常识的 prompt 较少，模型将基于先验知识去边缘化未观测到的变量，从而导致信息失真。由于具有庞大数据训练量，即使经过人工监督学习和奖励机制调整，一些错误或者编造的信息会逃过人工智能审核机制，成为 ChatGPT 输出答案的隐患。尤其在语言生成能力和逻辑能力大幅提高的框架下，ChatGPT 会让虚构的事实看似合理化，增加人工智能审核的难度。此外，随着信息传播速度的加快，以及 CharGPT 具有大规模且快速生成流畅文本的能力，真实性未得到验证的信息可能在多个平台或网站快速散播，导致真实用户的发声或者正确的信息被淹没。

第二、在较长的会话中，由于训练数据的偏差和过度修正，ChatGPT 会过度强调某些短语或者句子，导致重复性高的问题。例如它会重申它是由 OpenAI 训练的语言模型，这可能源于训练者对模型回答全面性的优化。而且，ChatGPT 对多次调整输入措辞或尝试相同的输入指令也会很敏感。例如，给定一个问题，模型可以声称不知道答案或拒绝回答，

但在指令稍作调整后，ChatGPT 也会识别并回答。

第三、ChatGPT 的强大能力依赖语料库、数据量的抓取和复杂的训练过程，训练成本和所需算力的成本都很高。如果数据库的收录内容质量不高或者数据量不够大，将会影响生成文本内容的质量和精细度，而且 ChatGPT 模型训练和优化过程较为复杂，需要专业的人员进行操作，训练成本和所需算力的成本都很高。最重要的是，ChatGPT 模型依赖于大规模离线语料进行训练，往往不能充分接受并采用在线提供的即时信息，难以理解对话中提及的因果关系，也无法基于已有信息进行推测，这距离人类举一反三的能力相差较远。

（二）发展瓶颈：人工智能的安全性和伦理约束

ChatGPT 本身的缺陷或许可以通过收集更多、更丰富的语料库，提高训练和优化的效率和质量，以及开发人工智能检查和修改的工具来改善，但是更深层次的 ChatGPT 引起了人们对 AIGC 行业中安全性、伦理约束和创造力的思考。由于 RLFH 并不能完全避免 ChatGPT 训练库中学习到的不道德或有偏见的回答，也会导致在模糊提示或引导回答的过程中让 ChatGPT 输出一些有害信息，导致输出结果的安全性降低。由于人工智能缺乏对伦理和常识的价值判断能力，也没有有效的约束方式，一旦模型存在不安全输出的可能性，ChatGPT 将容易被滥用。因此，为了提高 ChatGPT 输出内容的真实性和安全性，减少或拒绝有害信息的输出，在 ChatGPT 模型中添加限制或内置“内容安全过滤”模块是必要的。目

前 OpenAI 正在进行相关研究，增强 GPT 系统对用户意图的理解，并视情况筛选指令执行，推动自然语言交互工具的安全性提高。此外，在创造性、创作伦理和知识产权等方面并未形成有效界定。在数据挖掘、大规模计算、统计、多线程工作等数据处理分析领域，人工智能有着人类不可比拟的优势，但是以“创新和感知”为基础的创造过程是机器学习和模型难以训练的。目前 ChatGPT 能够在用户的引导下快速生成小说、诗歌、散文、编程等需要创造力的内容，或许将对创作者和以版权为基础的行业造成冲击。文本生成的过程是基于数据库内容的学习，这是否会构成对被抓取作品的侵权，ChatGPT 生成的文本内容是否具有著作权，是否属于该用户等等一系列问题的答案尚不明确。

（来源：《聊天机器人顶流 ChatGPT，开启自然语言处理领域新篇章》《AIGC 投资机会梳理：ChatGPT 快速流行，重构 AI 商业模式》）

ChatGPT 的技术发展路径

ChatGPT 的名称来源于它所使用的技术架构 GPT，即 Generative Pretrained Transformer，是一种强大的生成式预训练语言模型，能够完成复杂的自然语言处理领域（NLP）的任务，例如文本生成、机器翻译、代码生成、问答、对话 AI 等。GPT 模型在上述任务中并不需要监督学习，但模型训练过程需要庞大的训练语料、模型参数和强大的计算资源。在结构上，GPT 基于堆叠的 Transformer 组件进行编解码，通过提升训练语料的规模和质量、提升网络参数数量来完成 GPT 系列的迭代过程。近五年来 GPT 的发展过程也证明了模型能力的提高与参数量和预训练数据量有直接关联。

表 2　GPT 三代的对比

模型	发布时间	参数量	预训练数据量	pfsdays	消耗资源
GPT-1	2018 年 6 月	1.17 亿	约 5GB	0.96	在 8 个 GPU 上训练一个月
GPT-2	2019 年 2 月	15 亿	40GB	7.86	在 256 个 Google Cloud TPU v3 上训练一周
GPT-3	2020 年 5 月	1750 亿	45TB	3640	在 8 个 GPU 上训练一个月

资料来源：人民数字，品玩，中国银河证券研究院

一、GPT 初代：无监督的预训练结合有监督的模型微调

2018 年，在自然语言处理领域（NLP）刚兴起时，OpenAI

就推出的初代 GPT，它的运行逻辑是：先通过无标签数据学习生成语言模型，并能够运用于一些与有监督任务无关的 NLP 任务中。此后再根据特定的下游任务进行有监督的微调，提高其泛化能力。常用的有监督任务主要有：

- **自然语言推理**：判断两个句子的关系，是包含关系、矛盾关系或者中立关系；
- **问答和常识推理**：通过输入的文章和若干个问题及其候选答案，输出每个答案的预测概率；
- **语义相似度**：判断两个句子是否语义相关；
- **分类**：判断输入文本的指定类别。

在经过有监督的微调后，GPT-1 的泛化能力会得到明显提升，且随着训练次数的增加，GPT-1 的性能逐步提升。但是初代 GPT 仅仅使用了解码器部分，其 transformer 结构中对于词向量的学习能力得到发挥，能够实现较好地语言理解，适用于文本生成领域，但在通用语言和会话交流方面，还有较大的欠缺。

二、GPT-2：扩展了网络参数和数据集，进行多任务学习

相较于初代 GPT，2019 年推出的 GPT-2 整体上结构和设计没有变化，但学习目标是使用无监督的预训练模型作为有监督学习的任务，其核心逻辑在于让所有监督学习成为无监督语言模型的子集。换言之，GPT-2 可以在数据量足够丰富且模型容量足够大时，通过训练语言模型就能够完成有监督学习的任务。实际训练中，GPT-2 和 GPT 初代不同点在于：

（一）更广泛的信息来源：在预训练时扩充 NLP 任务的数据集到 40G;

（二）更庞大的网络参数：将 transformer 的层数增加到 48，隐层（hidden layer）维度扩展到 1600，实现了 15 亿的参数量;

（三）不再针对不同的任务建模微调：将机器翻译、自然语言推理、语义分析、关系提取等 10 类任务统一建模为一个分类任务，让模型在预训练中自己识别任务。

在性能方面，GPT-2 可以在多个特定的语言场景下良好地完成 NLP 任务，除了语言理解能力外，还可以胜任翻译生成、故事编写、总结摘要等。这些能力基于海量数据和大量参数训练的词向量模型，不需要监督微调和额外的训练即可迁移，基本实现了元学习。同时，GPT-2 能够让数据库中词向量包含的信息在多任务中通用，实现了信息脱离具体的 NLP 任务存在，也证明了随着模型容器和数据量扩充，GPT 的无监督学习具有很大的提升空间。

三、GPT-3：海量参数，成就最强大的语言模型

对比 GPT-2，2020 年推出的 GPT-3 最显著的特征是庞大的数据量和参数投入，整体训练过程耗资 1200 万美元，投入数据量达上万亿，模型参数量达到 1750 亿。虽然 GPT-3 延续了前两代 GPT 的技术架构，但改变了“大规模数据集预训练+下游数据标注微调”的方式，采用情境学习来提高模型对话输出的性能。基于情境学习对于模型的引导，GPT-3

在示例学习中提升回答的准确性。在训练过程中，few-shot learning 将提供 10—100 个示例和任务描述供模型学习；one-shot learning 提供 1 个示例描述；zero shot 则不提供示例，只是在测试时提供任务相关的具体描述。这三种学习方式的效果与模型容量成正相关，且多个示例学习的增强效果高于单个示例或不提供示例。换言之，在超大模型的训练下，GPT-3 匹配正确答案的准确率大幅提升。在现存大量语言模型中，GPT-3 的规模和语言能力几乎是最强大的。它能在不做微调的情况下，在一些传统的 NLP 任务中表现得更好，包括实现闭卷问答、模式解析、纯语言建模、机器翻译等；在新的领域，GPT-3 将 NLP 的应用扩展到缺乏足够训练数据的领域，例如在开发程序代码、文章生成和信息检索领域取得了实质性的进展。此外，在 UI 设计、图像生成和艺术创作等领域，GPT-3 的功能也更加强大，可以不经过微调就补全图像样本、或者实现简单的视图交互设计，将应用领域从语言处理领域逐渐拓宽，实现了从语言到图像的转向。然而，GPT-3 在推理和理解能力上还有较长的路要走。在自然语言推理（NLI）中重点关注句子之间的关系，由于 GPT-3 的阅读理解性能存在一定缺陷，在 NLI 任务中表现不佳；类似的，在物理、科学的常识推理技能表现中也存在一定问题。

四、InstructGPT 和 ChatGPT：更好地遵循用户意图、更少的虚假信息

相较于 GPT-3，OpenAI 在 2022 年初发布了 InstructGPT。

该语言模型在 GPT-3 的基础上进行微调，并在工作原理上增加了对齐研究，强化 InstructGPT 模型的语义理解；同时，通过“基于人类反馈的强化学习（RLHF）和监督学习”来提高输出质量。具体地，开发人员可以将训练划分为三个阶段：

第一阶段：冷启动阶段的策略模型。随机抽取用户提交的指令或问题，即 prompt，并进行专业的人工标注，用这些指定的 prompt 和高质量答案共同微调 GPT-3.5 模型，使之初步具备理解输入指令或问题的能力。

第二阶段：训练回报模型。在第一阶段生成的众多结果中，根据结果质量由人工标注排序并作为训练数据，通过监督学习中的匹配排序训练回报模型对语言模型预训练的输出结果评分，回答质量越高，分数越高。

第三阶段：采用强化学习来增强预训练模型的能力。利用第二阶段学好的 RM 模型更新预训练模型的参数，不断从 prompt 库中抽取新命令，通过 PPO（Proximal Policy Optimization）算法生成回答后，循环执行第一到三阶段进行强化训练，最终鼓励 LLM 模型能够输出更高质量的回答。

虽然 InstructGPT 的参数量仅为 13 亿左右，相比于 GPT-3 缩小了 100 倍以上；但在遵循指令方面，能够更好地遵循用户意图，将有害的、不真实或者有偏差的信息输出最小化。在优化的模型上，ChatGPT 基于 InstructGPT 进一步改进，在模型结构和训练流程上遵循上述方式，但收集和标注数据的方式上发生了变化。

InstructGPT 模型需要先完成类似<prompt，answer>的输入、输出匹配，取得多个匹配结果后再跟模型的预训练数据对比，在第二阶段的 RM 中只有奖励、没有惩罚机制；而 ChatGPT 则是在输入 prompt，模型输出多个 answer 后，直接对输出结果进行人为排序，根据排序后的结果让模型完成预训练中从最优到最劣的排序。通过采取监督学习的方式让模型学习人类排序的方式。

（来源：《聊天机器人顶流 ChatGPT，开启自然语言处理领域新篇章》）

ChatGPT 未来的应用场景

作为人工智能的一次新发展，ChatGPT 的推出加速应用场景扩容，正在“掀起新一轮 AI 革命”浪潮。目前 ChatGPT 的应用场景主要聚焦在跨境电商、游戏开发、教育等领域，随着算力的增加、应用程序的迭代，以及应用场景的扩展，ChatGPT 将赋能千行百业，可以预期的包括虚拟数字人、模型调优、服务型 AI 应用升级、组合式创新等。随着 ChatGPT 的快速普及，海量应用场景将不断解锁，催生出新的增长点。

ChatGPT 未来多样化的应用前景主要有：

（一）虚拟数字人。现在火热的数字人，需要类似 ChatGPT 这样的模型提供对话能力，才能让数字人具备有趣的灵魂，更好地陪伴和服务人。同时，该能力也可以嵌入到机器人身体内，让未来的人形机器人更聪明，更智能。

（二）模型调优。开发者可以利用 ChatGPT 的底层平台，根据不同行业和场景进行模型调优，创造出各类满足用户需求的丰富应用和算法工具，形成对话式 AI 的生态。如文本生成和 AI 助写工具 Jasper. ai 通过 GPT3 模型微调能够自动生成各种类型的文本，包括邮件、新闻文章、广告语、社交媒体帖子等。

（三）服务型 AI 应用升级。在教育、医疗、广告营销、电子商务、市场和战略咨询、企业服务、编写代码等专业服

务领域，成为更为专业的人类助手，不仅可以生成内容，还可以调用各种专业能力，甚至替代部分初级的专业工作。如微软推出了由 ChatGPT 提供技术支持的高级 Teams 产品，可以自动帮助参会者生成会议记录，即使没有参加会议，智能回顾功能也能帮助用户生成会议记录和要点。

（四）组合式创新。与其他模态 AI 工具的组合式创新，ChatGPT 同文生图、文字生成视频、甚至未来直接生成 3D 模型的工具集成，可以带来 UGC 内容的极大丰富，成为工业化的核心引擎。未来，ChatGPT 与更多的 AI、云计算等信息技术的集成创新，将创造改变生产力曲线的工具，成为经济发展新动力。

（来源：《一文读懂：有关 ChatGPT 的十个问题》）

编辑部地址：南宁市体强路 18 号广西信息中心 1412 号房
联系电话：0771-6113592
电子邮箱：dsjyjs@gxi. gov. cn
网址：http：//gxxxzx. gxzf. gov. cn/

扫描二维码获取
更多决策参考信息