

MEMORY

空 · 每次清零

B站/公众号/YouTube: 唐国梁Tommy

官网 TGLTommy.com

第 100 次

用过一百次的它

~~本该 越用越强 ↑~~

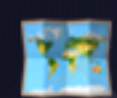


零成长

第 1 次

刚上手的它

说得直白一点 — 它每次醒来都**失忆**



本系列 · 路线图

从第一性原理出发，五个基本问题依次想清楚



⚠ 隐藏条件：第三步必须记得「项目资料」已改名为 Agent CL



聊天记录

写进提示词

改模型权重

本系列要追问的第一个问题

什么才算 Agent 持续学习?

🔍 拆开来看 · 今天的 Agent = 固定模型 + 工具 + 上下文 + 循环



● 会话进行中 = 连续工作的助手



🔄 上下文清空 = 回到原点

— 先区分三个常被混用的概念 —

① 状态延续

定义
知道“刚刚发生了什么”

例子
当前打开哪封邮件、标签叫什么

时间尺度
当前任务

② 记忆

定义
离开上下文后，未来能找回

例子
下周还记得用户不喜欢凌晨开会

时间尺度
跨会话

③ 学习

定义
未来新任务更快 / 更稳 / 更准

例子
能力发生可测量的改善

时间尺度
跨任务 能力↑

⚠ 光会“保存”不算数 —— 关键是能力发生可测量的改善

🧠 传统 Continual Learning · 灾难性遗忘

■ 任务 A · 原有能力 ■ 任务 B · 新训练 (覆盖 A)

任务 B 覆盖

任务 A 能力

⚠ 传统 CL: 怎样避免 B 的训练覆盖 A 的能力?

这是重要问题, 但对 Agent 来说, 这还不够 →

🎯 Agent 持续学习 · 更完整的定义

🧠 不忘记过去

=

只是一半



更完整的定义 —

随环境与经验不断变化

持续提高未来任务的
完成能力



arXiv · 2026.07 · 刚上线

统一视角

When Does Continual Learning Require Learning?

Authors et al. · 机构

3 类内部组件 → 4 个写入位置



记忆与状态一分为二 —— 一条经验，至少可以写入 这 4 个地方 →



一条经验 —— 至少能写到 四个地方

1 当前上下文 Current Context

存什么 临时状态 · 「正在处理哪封邮件」

✓ 更新快 · 易撤销

✗ 寿命短 · 容量小

2



外部记忆

External Memory

存什么 具体事实 · 用户偏好 · 历史事件

✓ 可精确编辑

⚠ 靠写入 + 检索质量

一条经验

写到哪里？

3 技能库 / Playbook Procedural Skills

存什么 「以后类似的事该怎么做」

e.g. 提交表单前，检查字段映射和最终状态

程序性经验



4



模型参数

Model Weights

何时 需广泛复用的新能力 / 反复学不会某类推理

微调 · 蒸馏 · 强化学习 → 改权重



带着这套底子，我们继续

带着「什么时候该动权重」这个判断，再往下看
这四个位置，各有各的成本和风险

▶ 接着看：四个位置到底怎么权衡取舍

📖 这套权衡先记一个轮廓 · 后面用一整集专门展开

Agent 持续学习 · 最难的一步 —

与其说是 ~~「如何更新」~~



不如说是 —

**判断这条经验，
究竟该写到哪里？**

?

当前上下文

外部记忆

技能库

模型参数

Agent 到底有没有学会？至少问三个问题

GEM

标准度量

当前表现 · 前向迁移 · 后向迁移

经典持续学习研究 GEM 定义 · 2026 论文沿用同一套指标

① 当前表现 Current Performance

同一个任务重试，
它会做得更好吗？

⚠️ 最弱标准：可能只是记住了答案

证据强度



最弱证据

② 前向迁移 Forward Transfer

相似但没见过的新任务，
过去经验还有用吗？

✓ 更强证据：形成可复用能力

证据强度



最强证据

③ 后向迁移 Backward Transfer

学了新经验之后，
旧能力有没有被破坏？

🛡️ 守护旧能力：学会新网站 ≠ 忘掉旧
工具参数

证据强度



守护能力

🎯 只看「第二次成功了」远远不够 —— 合格评估要同时看：当前学习 · 未来迁移 · 过去能力保留



泛化测试 —— 换掉表层，方法还成立吗？



换一个用户名

new username

✓ 方法仍有效



换一家网站

new website

✓ 方法仍有效



改变按钮文案

new button text

✓ 方法仍有效



方法仍有效 = 经验中的结构被保留下来

🕵️ 四种“伪持续学习”

看起来在学，其实是障眼法

①



上下文续写 伪 x

context continuation

- 历史还在窗口里，它只是“继续读”

②



答案缓存 伪 x

answer caching

- 记住答案，换个题面就废

③



无限回放 伪 x

infinite replay

- 旧轨迹塞满提示词，成本随历史线性膨胀

④



评测泄漏 伪 x

evaluation leakage

- 同一批题既当练习又当考试

🧩 两个反向命题：系统 $\neq$ 模型

命题一

基础模型 完全不变

+ 记忆 / 技能 / 工具编排



仍可形成 学习系统



命题二

模型权重 不断更新

但 无未来迁移 / 破坏旧能力



不算成功的持续学习



🎯 Agent CL 是系统问题，不只是模型问题



本集 · 第一性结论



~~不是让系统永远保留历史~~



而是让过去经验能够以合适的形式进入系统
对**未来能力**产生**持续、可验证**的改善



正好相反：记忆越多 →

噪声

冲突

过时信息

也越多

点击

失败

过时

日志

矛盾

冲突

轨迹

观察

状态

▶ 下集预告

EP02

Agent 记忆的第一性原理

为什么记住一切，反而可能什么也学不会

版权声明

唐国梁 Tommy 原创出品 | 熵智未来（深圳）科技有限公司版权所有。保留所有权利。

本课程及配套资料，包括但不限于课程视频、PDF 文档、课件、代码、图表、示例项目、知识库文档及其他学习材料，仅供购买本课程的用户本人学习使用。未经版权所有者书面许可，任何个人或机构不得以任何形式对本课程及配套资料进行录制、复制、传播、上传、公开分享、分发、转售、改编、翻译、汇编，或用于商业培训、企业内训、商业化产品、知识库建设、数据集构建、人工智能模型训练、微调及其他商业用途。如发现侵犯本课程及配套资料相关权益的行为，权利人有权依法要求停止侵害、删除下架、赔偿损失，并追究相应责任。

本课程及配套资料中涉及的第三方开源软件、模型、代码、数据集、商标、图片及其他素材，仅在相关许可证允许范围内进行教学展示，其相关权利归原权利人所有。

侵权举报 / 授权合作: legal@tgltommyai.com

微信公众号: 唐国梁TGLTommy | 官方网站: TGLTommy.com (国内访问需科学上网)