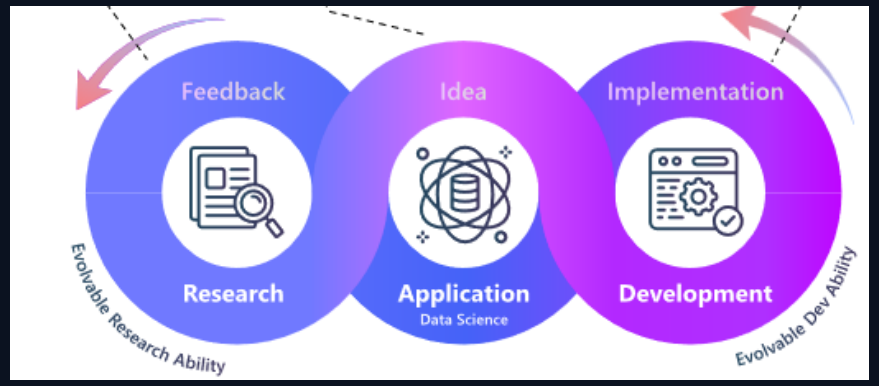
从电池数字孪生到自主研发：面向科学与工程的 Agentic Optimization



方樹楷 浙江大学

宁德时代 交流 · 2026.11

个人介绍

浙江大学 ZHEJIANG UNIVERSITY



方樹楷 博士

百人计划研究员 | 博士生导师

单位 信息与电子工程学院

邮箱 fsk@zju.edu.cn

研究方向
- 机器学习
- 生成式物理仿真和信号处理
- LLM多智能体系统
- 大规模高维时空序列

Morgan Stanley

達摩院 ALIBABA DAMO ACADEMY

Microsoft Research 微软亚洲研究院

RD-Agent

Fork 2k | Starred 15.3k

MarS

Fork 203 | Starred 1.9k

Agentic System 的边界与迷思：太多重复发明的名词

- “Fancy words are invented everyday… and combined randomly”

Perception

Structured feedback (logs, metrics, curves)

Reasoning

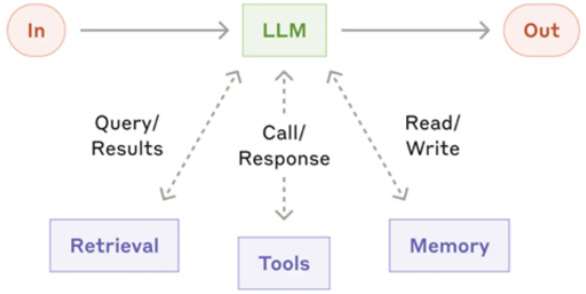
LLM-driven hypothesis formation

Action

Code execution, API calls, simulator runs

Memory

Accumulates outcomes · makes it evolving



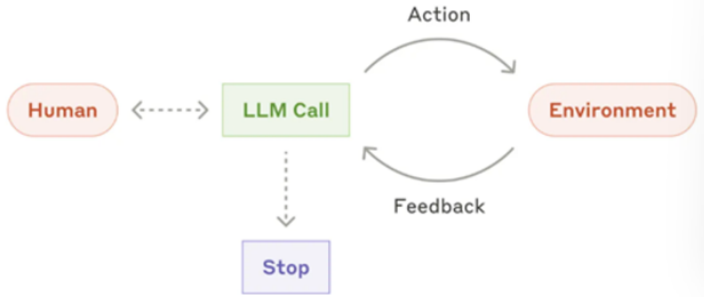
“Augmented LLM”



“evaluator-optimizer workflow”



“Orchestrator-workers”

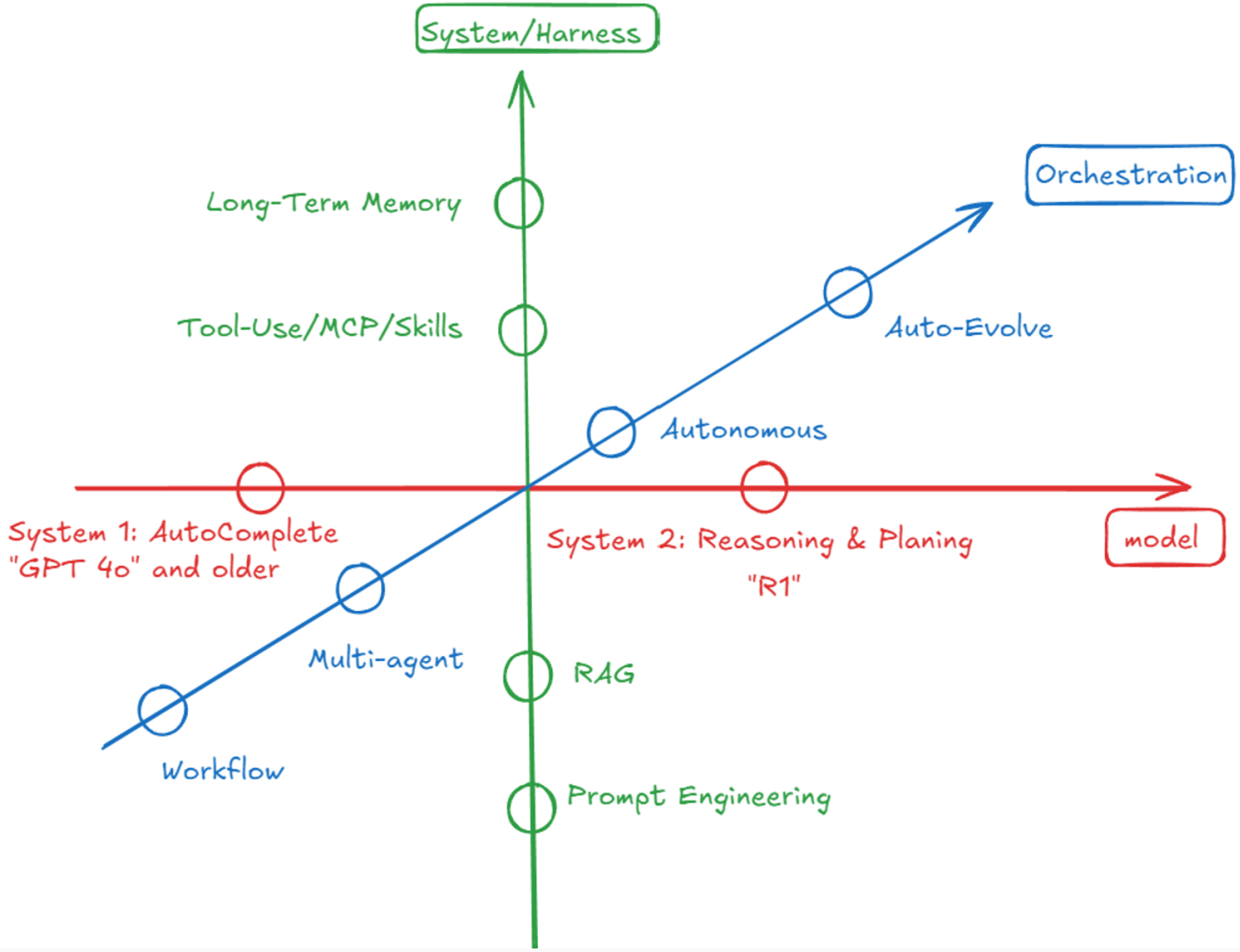


“Fully Autonomous”

Figs: “Building effective agents”, blog of anthropic

Agentic System 结构能力三个维度

- “Trying to sort out such fancy words..”



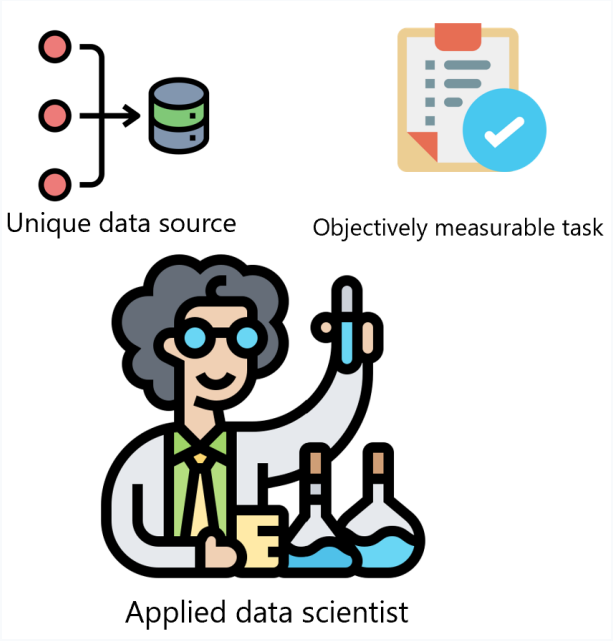
Fancy Enough!...?

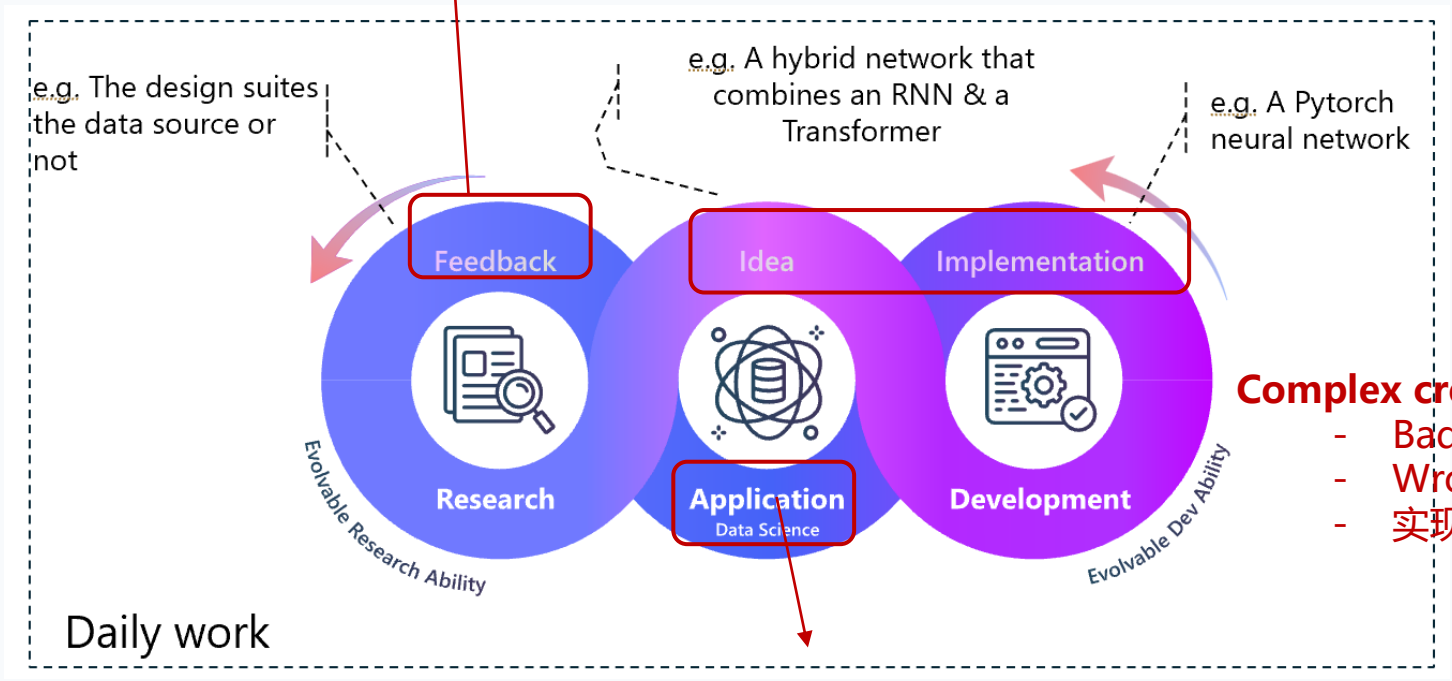
for tasks like
AI4Coding/GUI/Web:

- Clear Feedback (Yes/No)
- Short-Term Evaluation

工业级高价值科学&工程场景的边界

Non-trivial verifier: 异质、异步、多目标、多模态的反馈 （Beyond Yes/No）





Complex credit assignment:

- Bad Idea?
- Wrong feature?
- 实现有问题?

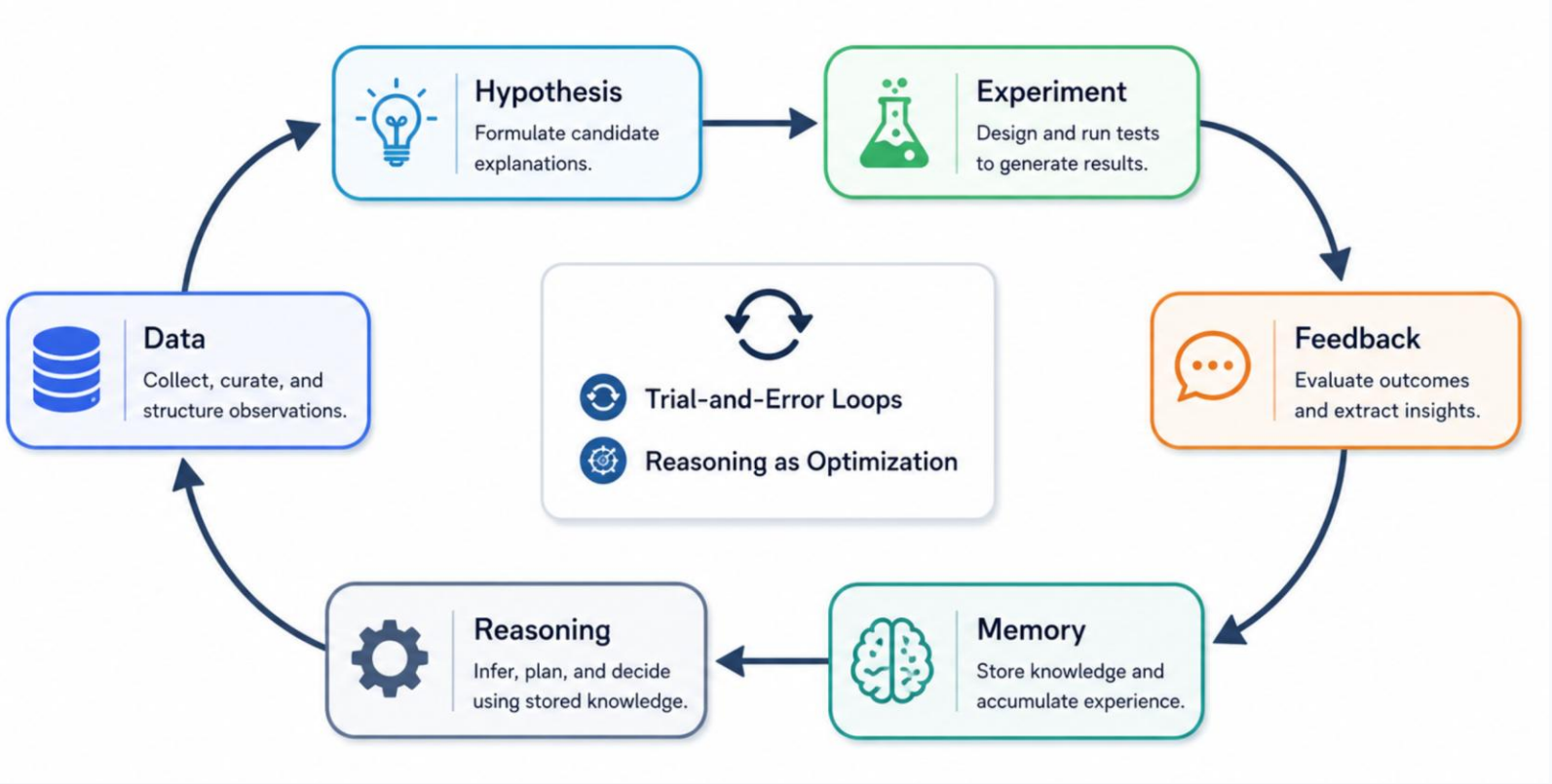
Multi-factor in loop:

长周期，高成本，多约束， 黑箱, 试错成本，合规风险

工业R&D与通用交互任务

维度	通用交互任务	工业R&D任务
反馈	明确、短期、用户可直接判断	多目标、长链路、包含日志/曲线/约束
评估	秒级到分钟级	分钟到小时，真实实验甚至更长
动作	网页、GUI、API等离散动作	代码、模型、因子、物理参数的连续空间
风险	重试成本低	错误归因困难，可能产生虚假进步
目标	完成任务	提升可复用的研究能力与研发吞吐

Agentic R&D Loop 的核心组件和设计原则



形式化视角

- 感知：结构化反馈
- 推理：诊断与假设
- 行动：实验或实现
- 记忆：跨轮次经验
- 验证：约束与可信评估

第一部分

工业场景数据驱动R&D范式

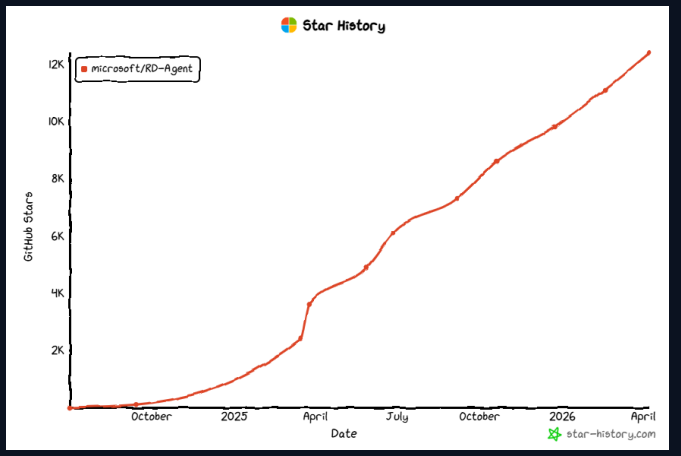
R&D-Agent：研究与开发解耦的自动化框架 (tech report arxiv. 2505.14738v2, 2603.01692v2)

Reasoning as Gradient：推理作为优化信号 (ACL 2026， arXiv:2603.01692)

核心问题：如何让反馈驱动可验证的研究迭代

RD-Agent

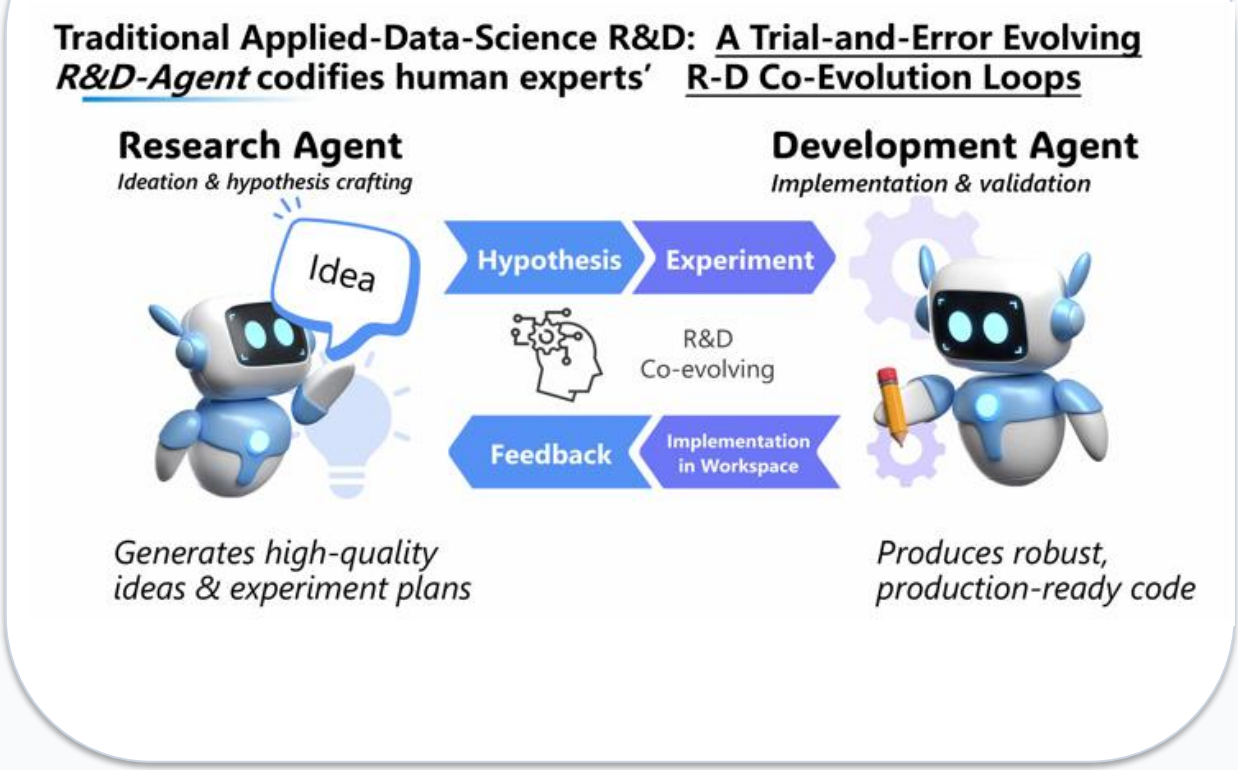
Fork 2k Starred 15.3k



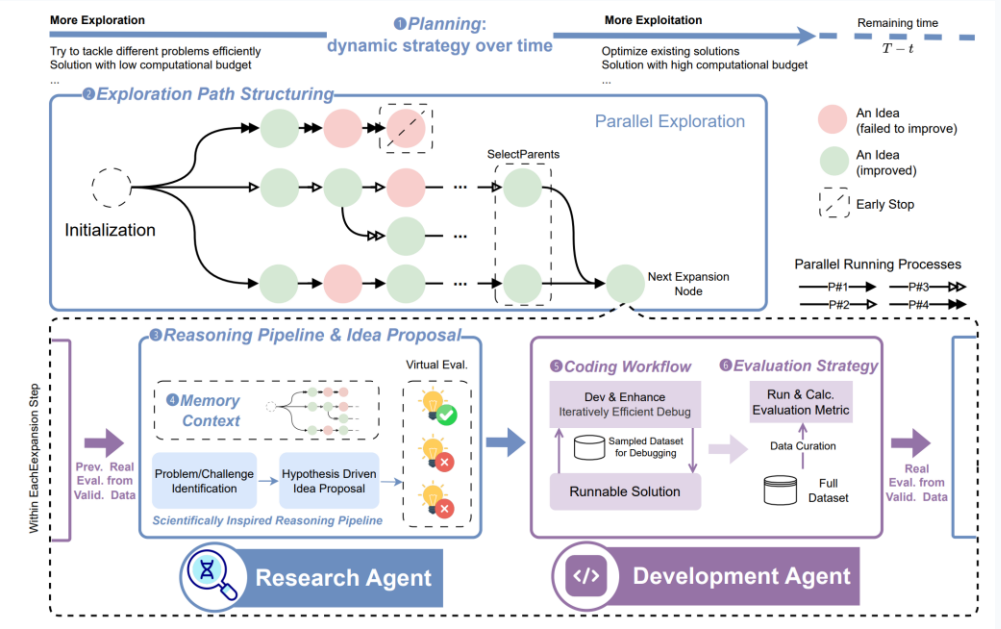
- https://github.com/microsoft/RD-Agent

R&D-Agent框架：化繁为简，双Agent框架

将机器学习工程拆解为研究-落地的两阶段流程。

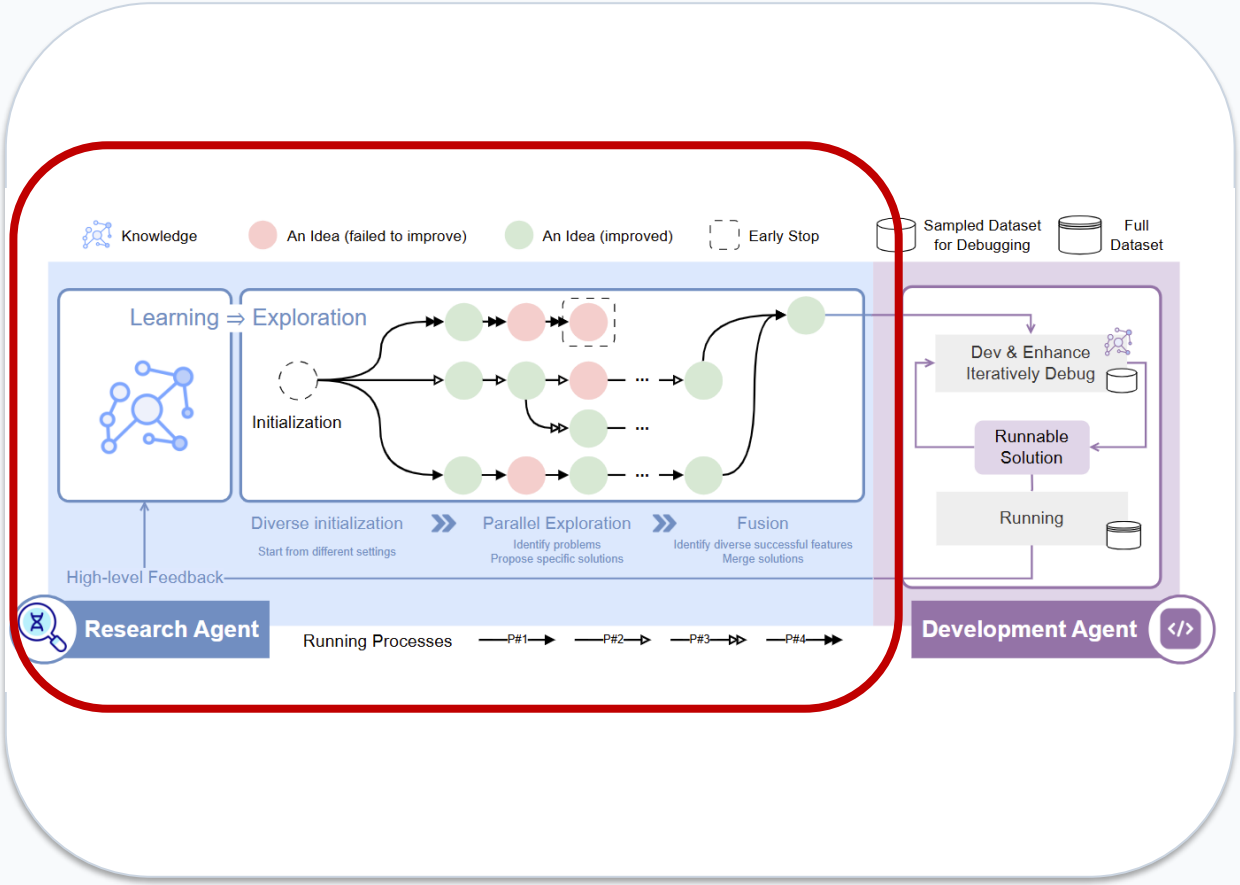


- Research Agent 负责规划、探索、记忆与假设形成。
- Development Agent 负责实现、调试与稳定评估。
- 共享记忆使多分支探索具有协同效应 + 协同进化。



研究阶段/Research agent： 更高效的探索

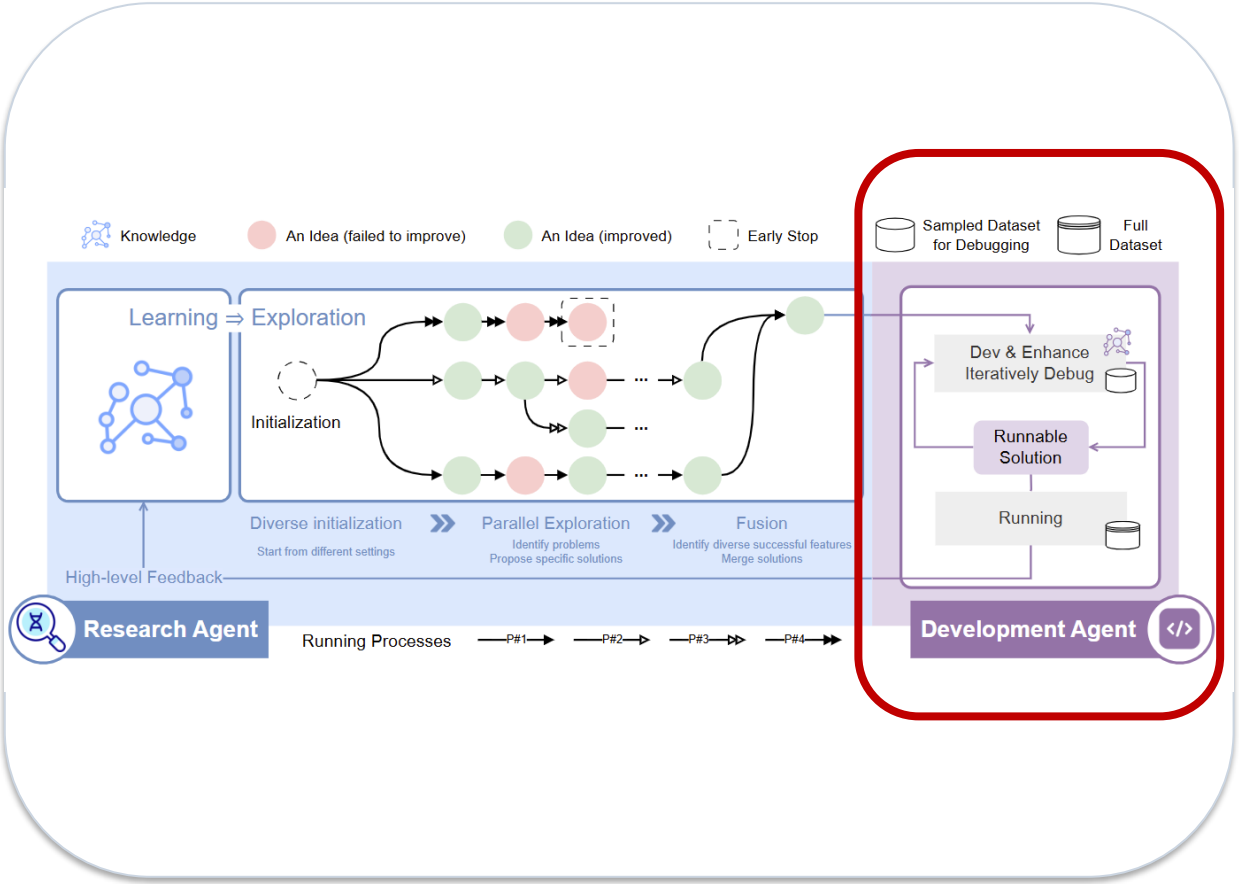
多路探索与结构化推理共同决定 idea 的质量。

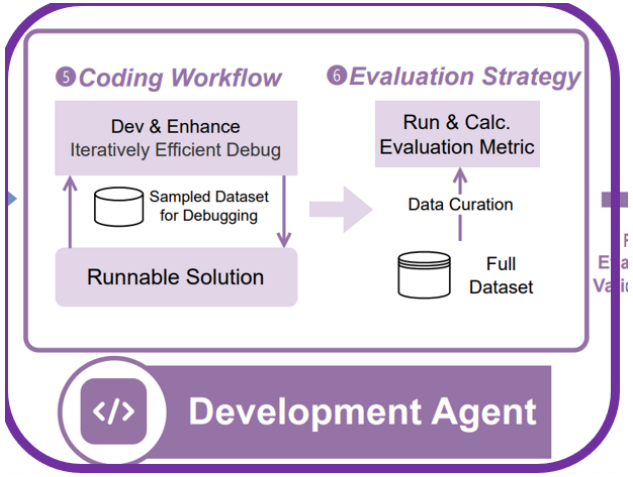


- 强制多样性避免所有分支过早收敛。
- 三步推理：问题识别、机制假设、具体改动。
- 高分经验通过记忆跨分支传播。

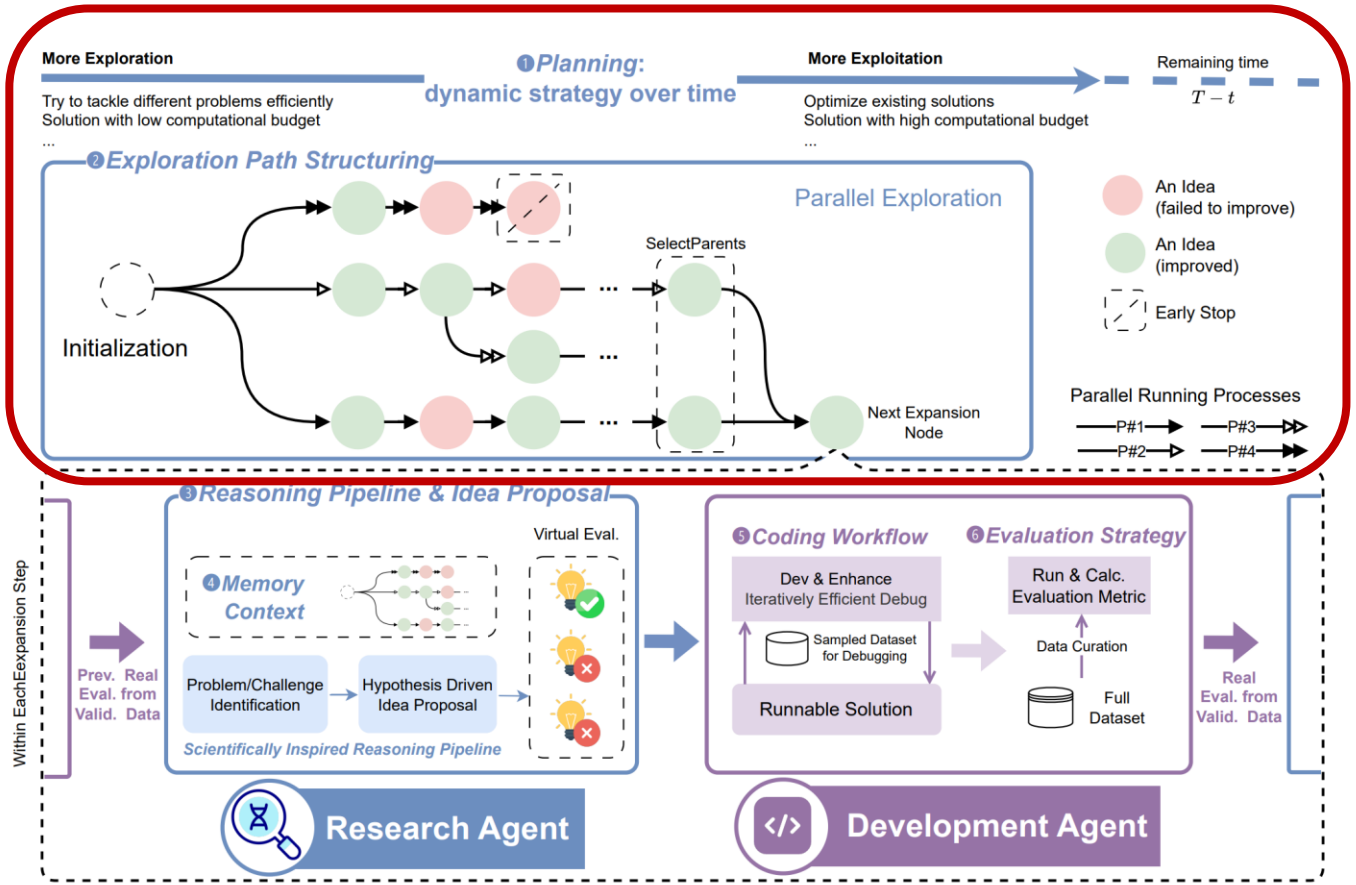
开发阶段/ Development agent： 沙盒与自检

在完整训练之前，进行充分的可行性与压力测试。





成本感知的探索路径规划



- 在整个探索流程的不同阶段，尝试不同风格的探索策略
- 及时早停
- 可作为更加复杂探索策略的接口

Prompt示例： 鼓励结构化， 但不把结构化写死； 鼓励使用工具 inner-loop 来debug

Scientific Hypothesis Generation —— Reasoning Pipeline Component

You are a research scientist formulating testable hypotheses. For each hypothesis, perform two main tasks: hypothesis proposal and rigorous five-dimensional evaluation.

Hypothesis Development Guidelines:

1. **Specificity & Decisiveness:** State exact, unambiguous changes. Avoid vague goals or alternatives.
2. **Testability & Actionability:** Describe implementable and measurable changes. Focus on single, unified conceptual improvements.
3. **Evidence-Based Reasoning:** Ground hypotheses in experimental history or domain knowledge.
4. **Implementation Feasibility:** Consider resource constraints and technical complexity.

Five-Dimensional Evaluation Protocol: Score each hypothesis (1-10) across:

- **Problem-Hypothesis Alignment:** How well the hypothesis addresses the identified problem
- **Expected Impact:** The estimated improvement after applying the hypothesis
- **Novelty:** Degree of innovation compared to previous attempts
- **Feasibility:** The ease of implementing the proposed hypothesis
- **Risk-Reward Balance:** The exploration-exploitation balance of the proposed hypothesis

Component Classification: Assign each hypothesis to: `DataLoadSpec`, `FeatureEng`, `Model`, `Ensemble`, or `Workflow`.

Memory-Enhanced Code Generation —— Memory Context Component

You are a grandmaster-level data scientist generating robust, debuggable code following systematic development process.

Important Context: You are working on sample datasets and your code will go through automated iterations. Design your code to be iteration-friendly with comprehensive print statements and clear debugging information to facilitate the automatic improvement process.

Memory-Enhanced Guidelines:

1. **Historical Learning:** Reference previous failed attempts and their feedback
2. **Pattern Reuse:** Apply successful patterns from similar tasks
3. **Error Prevention:** Avoid mistakes that occurred in previous experiments
4. **Performance Optimization:** Implement improvements suggested in historical feedback

Quality Assurance Requirements:

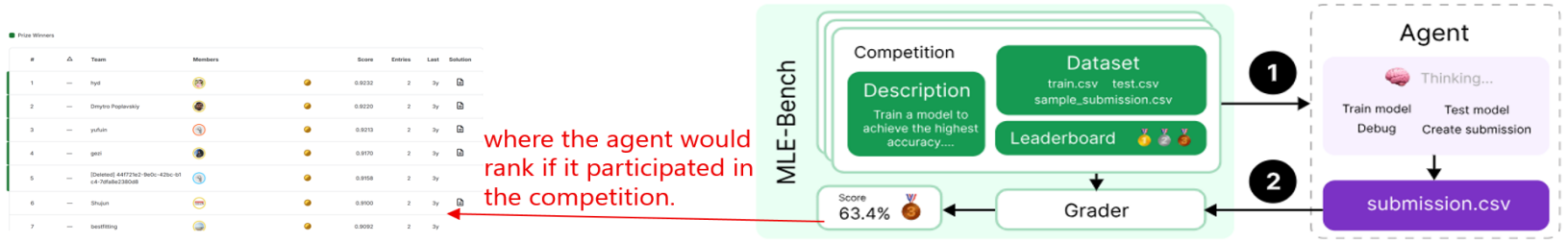
- **Debug Mode Integration:** Support `-debug` flag with data sampling and timing estimation
- **Structured Output:** Use print statements for progress tracking, avoid external logging dependencies
- **Reproducibility:** Implement proper random seed management and deterministic behavior
- **Resource Management:** Dynamic resource allocation and proportional data splitting

Open-AI MLE-Bench:

75个真实Kaggle竞赛上的端到端评估。

➥ MLE-Bench: the largest public ML-engineering benchmark

- 75 kaggle competitions crossing several domains published and open-sourced by OpenAI



- Industry span



- 覆盖CV、NLP、表格、时序与多模态任务。
- 任务要求特征工程、模型选择、调参、集成与调试。

- Task span
  - classification, regression, object detection, semantic segmentation, sequence prediction, QA...

MLE-Bench 评估

75个真实Kaggle竞赛上的端到端评估。

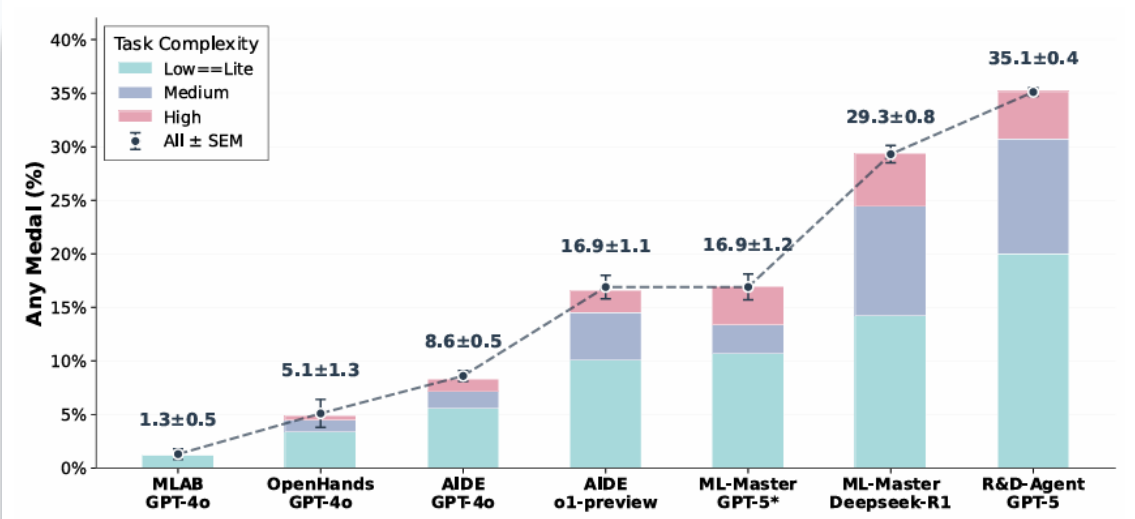
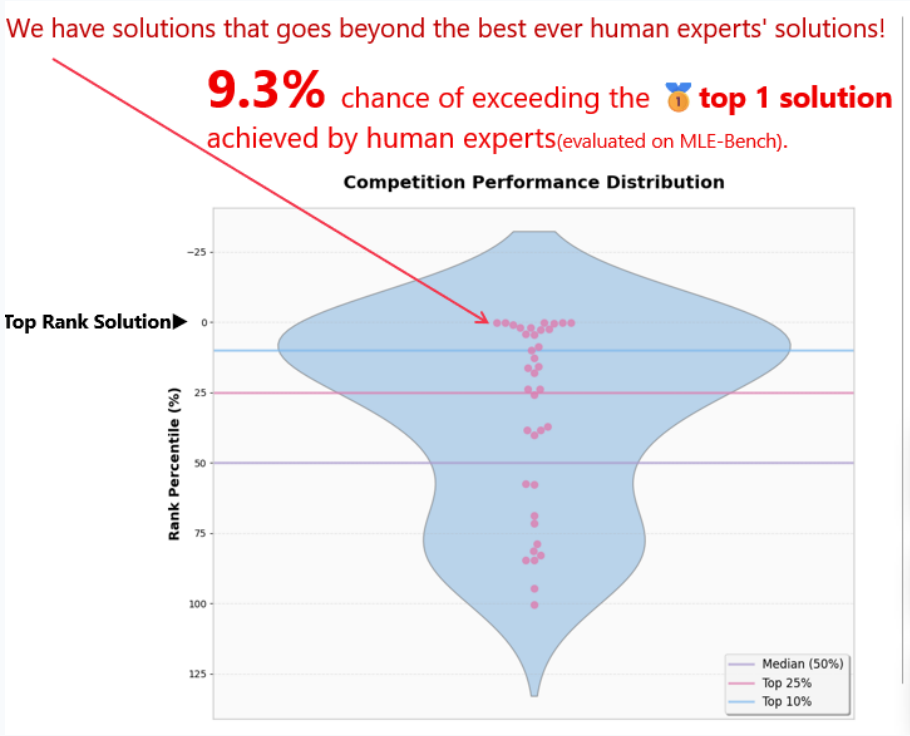


Figure 1: Agent performance on MLE-Bench. Stacked bars show any medal rates for Low==Lite (22 tasks), Medium (38 tasks), and High (15 tasks) complexity levels. The dashed line indicates overall performance (mean ± SEM). R&D-Agent achieves SOTA performance at 35.1 ± 0.4%. * indicates our re-evaluation of ML-Master within our environment.

35.1%
奖牌率

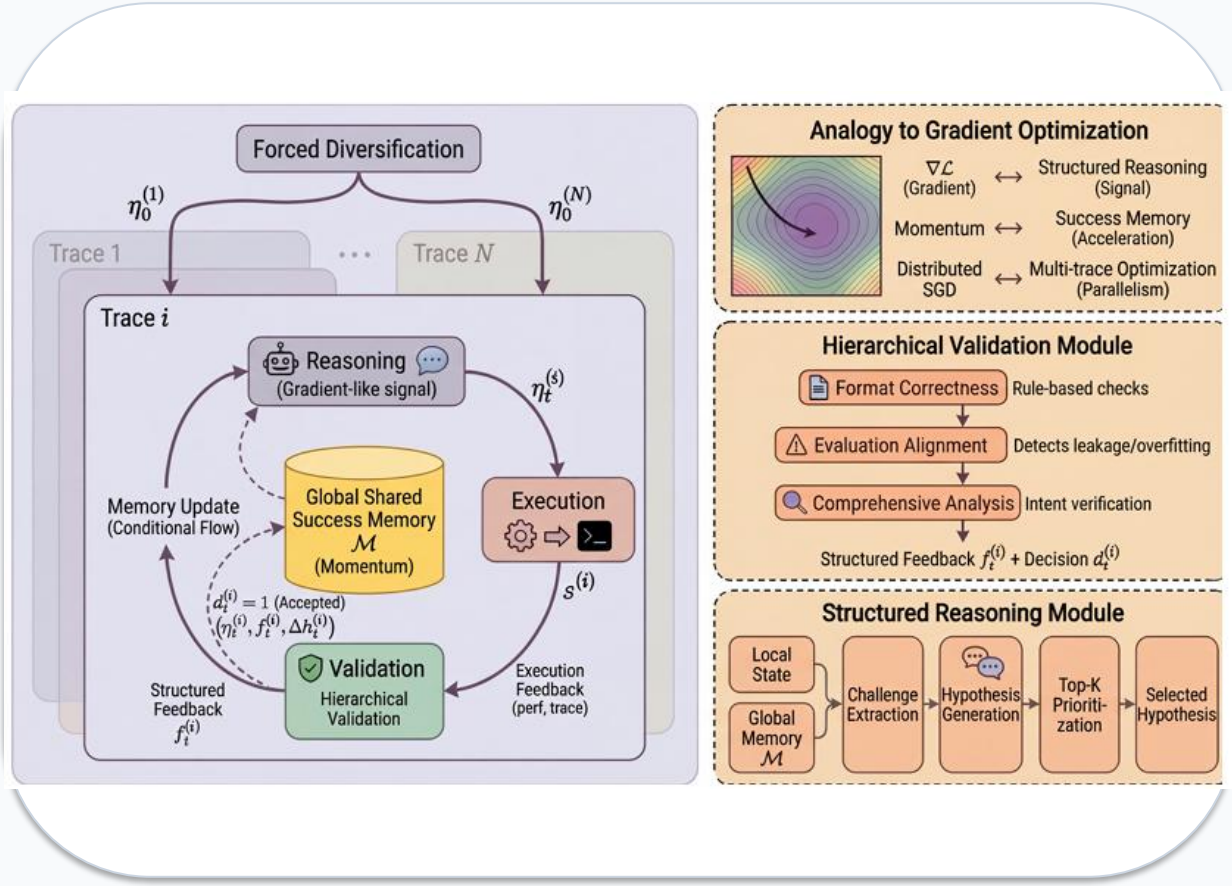
96%
有效提交率

13.8k
GitHub星标



更进一步: 如何用好大模型的推理能力——推理作为优化信号

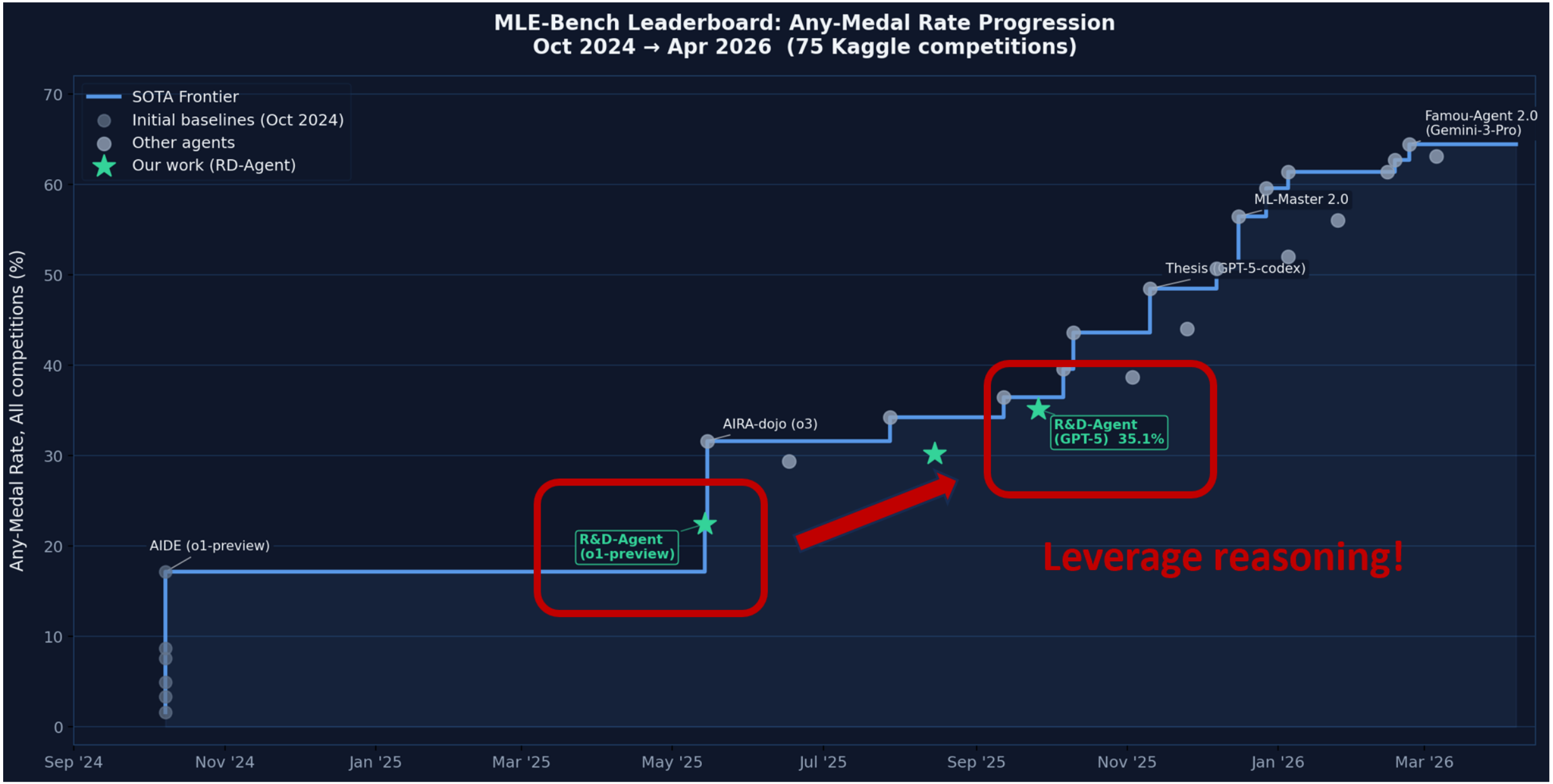
R&D Agent -> GOME 将诊断推理、成功记忆与多轨迹执行映射到优化器组件。



- 结构化诊断推理对应更新方向。
- 成功记忆对应动量。
- 多轨迹执行对应分布式优化。

Concept	GOME Component	Functional Role
Gradient ∇L	Structured Reasoning	Signal: decides how to update
Momentum	Success Memory	Acceleration via proven patterns
Distributed SGD	Multi-trace Optimization	Parallelism with knowledge sharing

Table 2: Analogy between GOME and gradient-based optimization.


MLE-Bench Leaderboard: Any-Medal Rate Progression
Oct 2024 → Apr 2026 (75 Kaggle competitions)
SOTA Frontier
Initial baselines (Oct 2024)
Other agents
Our work (RD-Agent)
Any-Medal Rate, All competitions (%)
0
10
20
30
40
50
60
70
Sep '24
Nov '24
Jan '25
Mar '25
May '25
Jul '25
Sep '25
Nov '25
Jan '26
Mar '26
AIDE (o1-preview)
R&D-Agent (o1-preview)
AIRA-dojo (o3)
Thesis (GPT-5-codex)
ML-Master 2.0
R&D-Agent (GPT-5) 35.1%
Famou-Agent 2.0 (Gemini-3-Pro)
Leverage reasoning!

第二部分

电池参数反演与物理仿真智能体

Battery-Sim-Agent | KDD 2026

从数据驱动的研发迭代，走向物理约束下的参数搜索

Battery-Sim-Agent: Leveraging LLM-Agent for Inverse Battery Parameter Estimation

Jiawei Chen*
Peking University
Beijing, China

Xiaofan Gui†
Microsoft Research
Beijing, China

Shikai Fang†
Zhejiang University
Hangzhou, Zhejiang, China

Shengyu Tao
Chalmers University of Technology
Gothenburg, Sweden

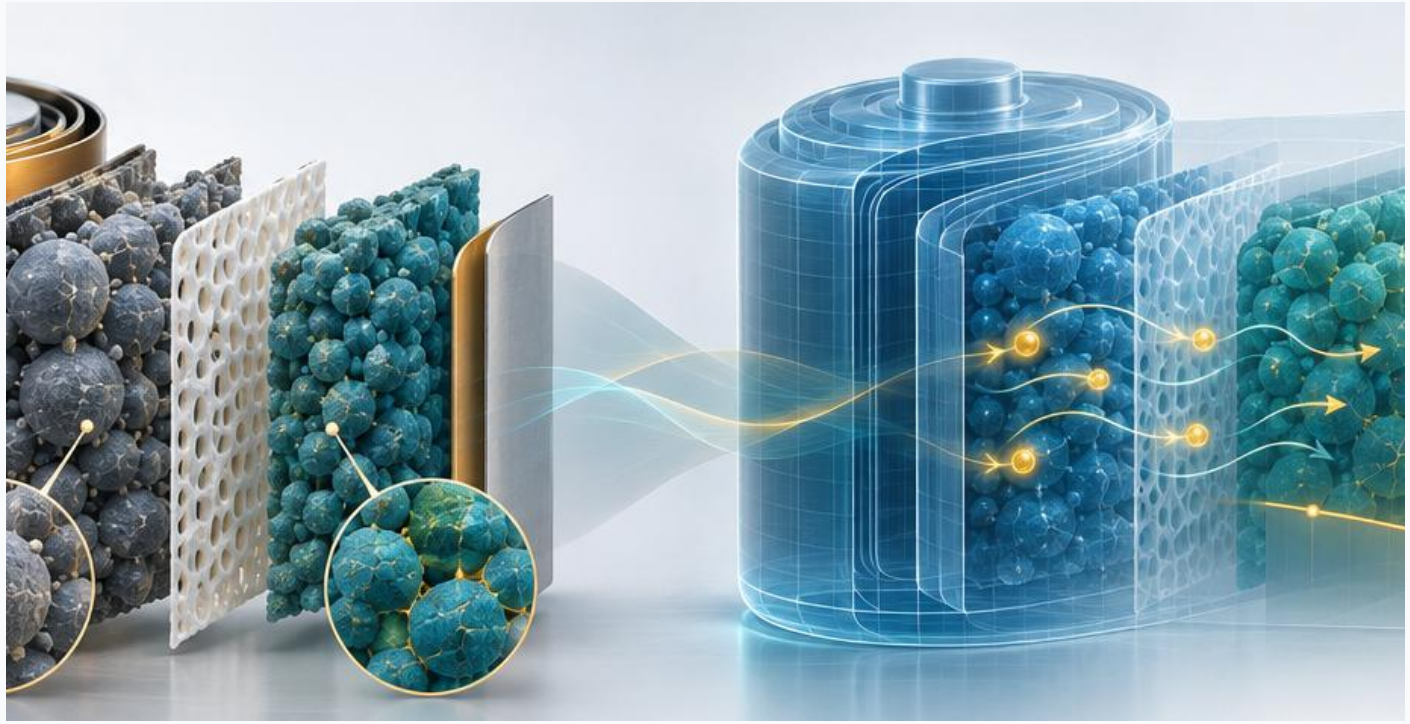
Shun Zheng
Microsoft Research
Beijing, China

Weiqing Liu†
Microsoft Research
Beijing, China

Jiang Bian
Microsoft Research
Beijing, China

为什么需要虚拟电池/数字孪生?

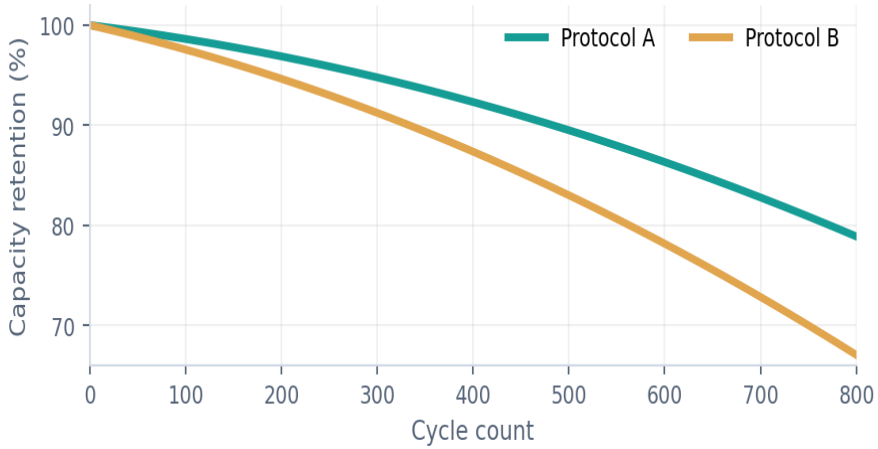
通过观测持续校准模型，预测循环衰减，并评估不同工况与管理策略。



物理电池 ↔ 观测数据 ↔ 可更新的模型 → 多循环预测与策略评估

循环衰减的模型预测

示意曲线 · 非实测数据



从模型标定到工程决策

- 多次充放电下的容量 / 性能变化
- 温度、倍率与充电协议的影响
- SOH / RUL 推断及策略模拟

Real2Sim的反问题：从少量宏观观测校准仿真器

已知：真实电芯在给定充放电工况下的电压、电流与容量；未知：与该电芯相匹配的模型参数。

正向仿真

待辨识参数 θ

结构 · 电化学 · 退化参数

→

DFN / PyBaMM

电化学正演模型

→

V(t) • I(t) • Q(t)

电压 / 电流 / 容量曲线

参数反演

少量真实电芯数据 + 已知工况

→

求解 θ*，校准仿真器

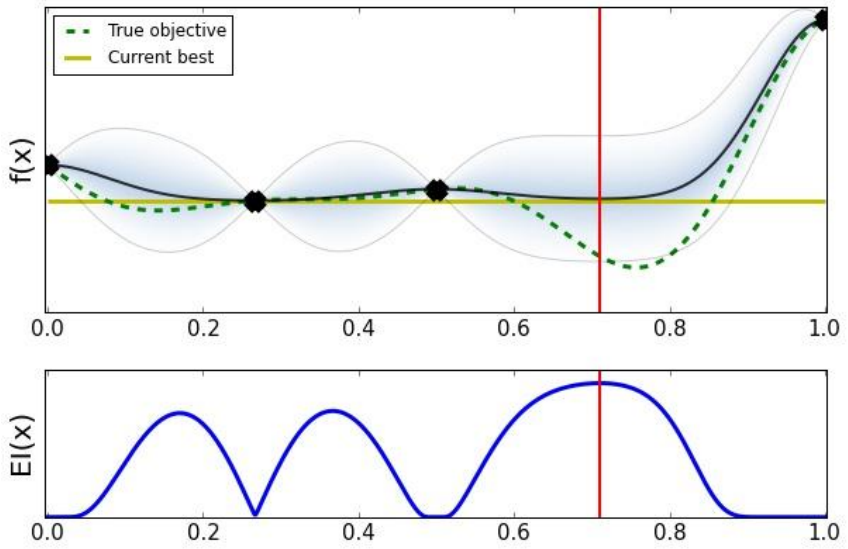
目标：在参数约束内，使仿真响应与真实观测相匹配。

$$\theta^* = \arg\min_{(\theta \in \Theta)} \Sigma_p \, d(F(\theta, u_p), y_p)$$ p：观测工况

传统黑盒优化：如何选取下一组参数?

贝叶斯优化建立响应模型后选点；遗传算法通过选择、交叉与变异更新候选种群。

贝叶斯优化

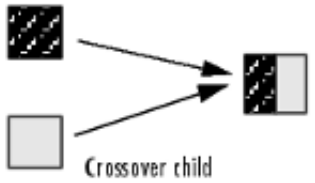


高维异质空间中，有限样本难以刻画耦合响应。

遗传算法



保留优良个体



组合父代参数



随机改变参数

种群评价需要大量仿真；参数组合还需满足物理约束。

图源：Emukit 官方教程；MathWorks — How the Genetic Algorithm Works

困难一：待辨识参数数量多、类型异质、强耦合

参数跨越结构、电化学与退化机制，直接测量成本高；不同参数的量级、边界和敏感性差异显著。

结构参数

电极厚度、孔隙率
颗粒半径、隔膜厚度

电化学参数

固相与电解液扩散系数
电导率、反应动力学参数

退化参数

SEI 反应速率
SEI 电导率、初始膜厚

给定工况与参数 θ → DFN / PyBaMM → 仿真曲线与实验观测的偏差

高维与强耦合

多个参数共同影响曲线
局部改善可能牺牲其他指标

异质性与尺度差异

不同单位、量级与物理边界
对倍率和循环阶段的敏感性不同

昂贵且不稳定的评价

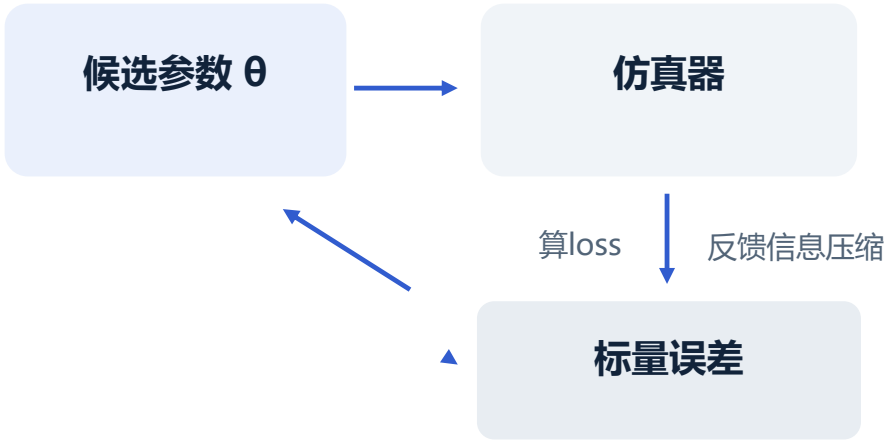
每次候选都要运行仿真
求解失败、非光滑响应与多解

优化目标：在物理约束下，同时匹配多个工况与多种响应。

困难二：一次仿真返回多模态、多目标反馈

电压曲线、容量偏差、充放电阶段和求解日志，需要共同解释，才能判断一次参数更新的效果。

常见黑盒反馈接口



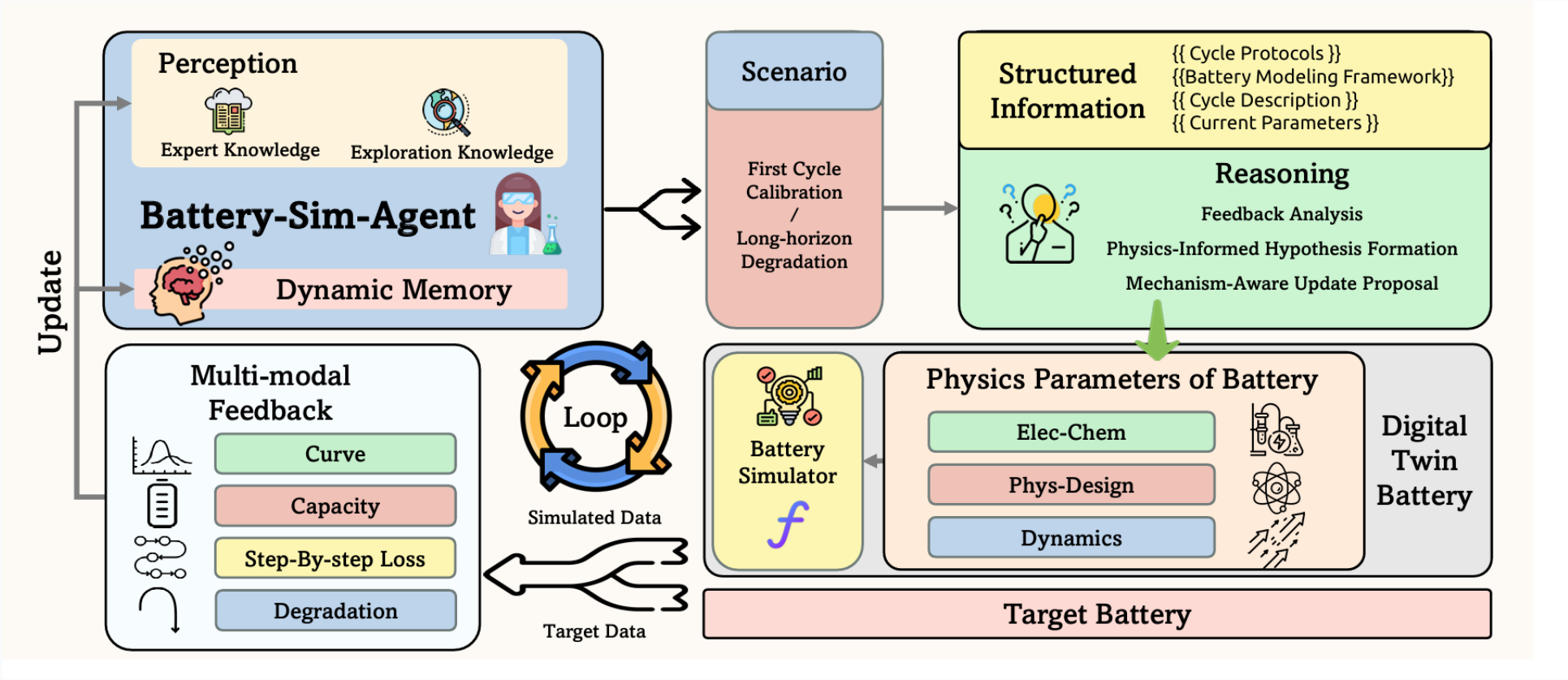
仿真返回的多类信息

曲线形态	CC / CV 阶段、平台偏差、斜率
多维目标	容量 Q、电压 V、电流 I 的不同残差
求解状态	失败日志、约束越界、数值不稳定
物理先验	参数敏感性、因果假设、经验记忆

优化难点：不同反馈的含义与尺度不同，压缩成总误差会丢失诊断信息。

Battery-Sim-Agent：用智能体组织参数反演

智能体解释仿真与真实观测之间的差异，形成机制假设，调用仿真器检验参数更新。



观测与仿真比较 → 结构化反馈 → 机理假设 → 受约束参数更新 → 记忆积累

创新点一：把多模态反馈接入可执行的优化循环

结构化曲线、指标和日志，结合领域先验输出受约束参数更新，并将结果写入记忆。



1 感知
曲线/容量/分阶段误差 + 仿真错误

2 推理
诊断差异并形成物理假设

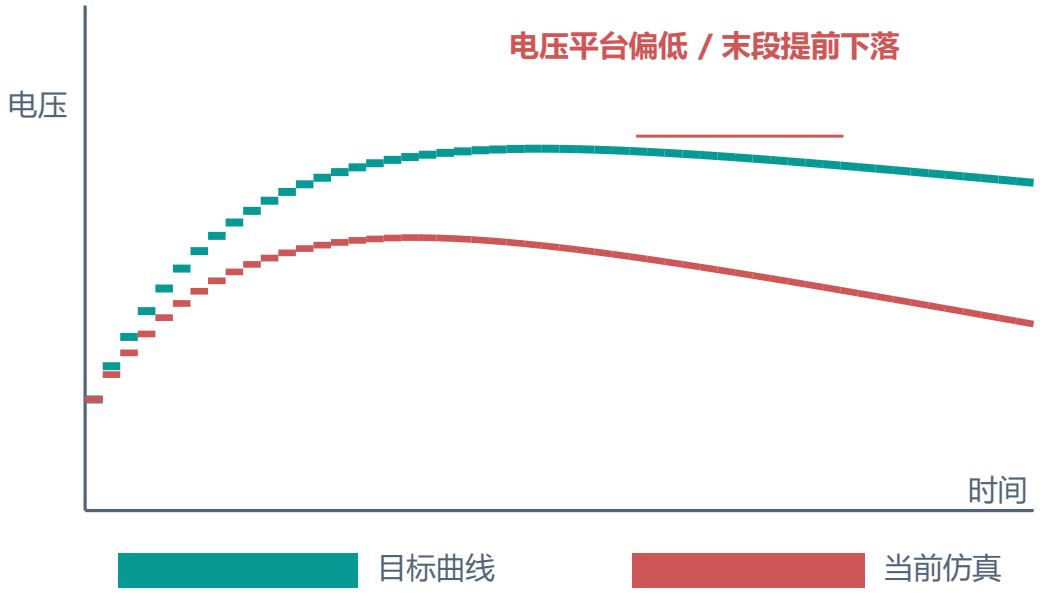
3 行动
输出机器可解析的参数更新

4 记忆
写入每轮假设、结果和副作用

创新点二：机制假设驱动参数更新

定位曲线偏差 → 提出电化学机制假设 → 选择相关参数 → 用下一轮仿真检验。

V(t) — 示意性曲线残差



① 诊断残差

平台高度、斜率与 CC / CV 区间并不一致

② 提出假设

例如传质受限或反应动力学参数不匹配

③ 更新参数

选择相关参数，生成有物理边界的更新

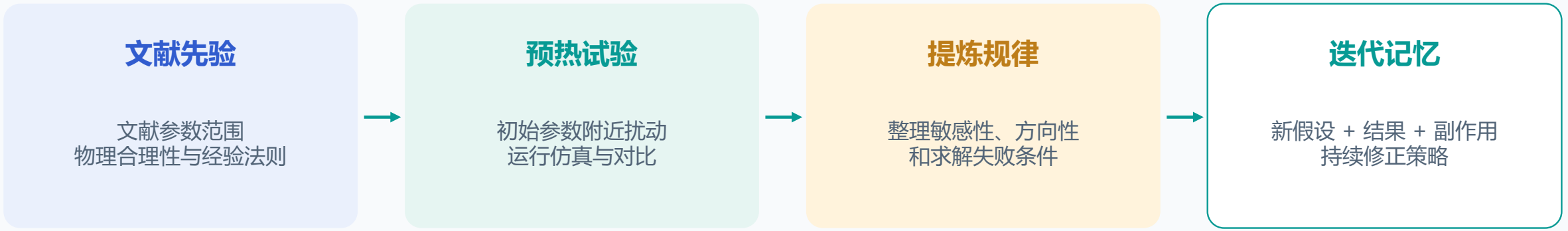
④ 仿真检验

重新调用 PyBaMM；记录改善与副作用

迭代机制示意

创新点三：知识预热与动态记忆

通过局部扰动积累参数敏感性，再将每轮的假设、改动和结果用于后续搜索。



示例：形成“局部敏感性知识”

对负极厚度施加 +10% 扰动 → 观察到容量上升；但高倍率条件可能出现仿真失败。

核心价值

减少重复试错
让后续动作利用累计证据

实验设计：用扰动参数构造“目标电池”

主 benchmark 使用仿真生成的宏观观测；缺少自有电芯与配套实测资源，采用公开电池参数设定构造受控任务。

公开参数集 θ_0

Chen2020、ORegan2022
Ecker2015、Prada2013
Marquis2019

→

构造目标参数 θ*

多参数组合扰动
或单参数大幅扰动

→

生成目标观测 y*

用 θ* 与给定工况仿真
获得电压、电流、容量
作为“真实电池宏观观测”

→

从 θ_0 开始反演

只向优化器提供目标曲线
通过反复仿真校准参数
再与已知 θ* 对照

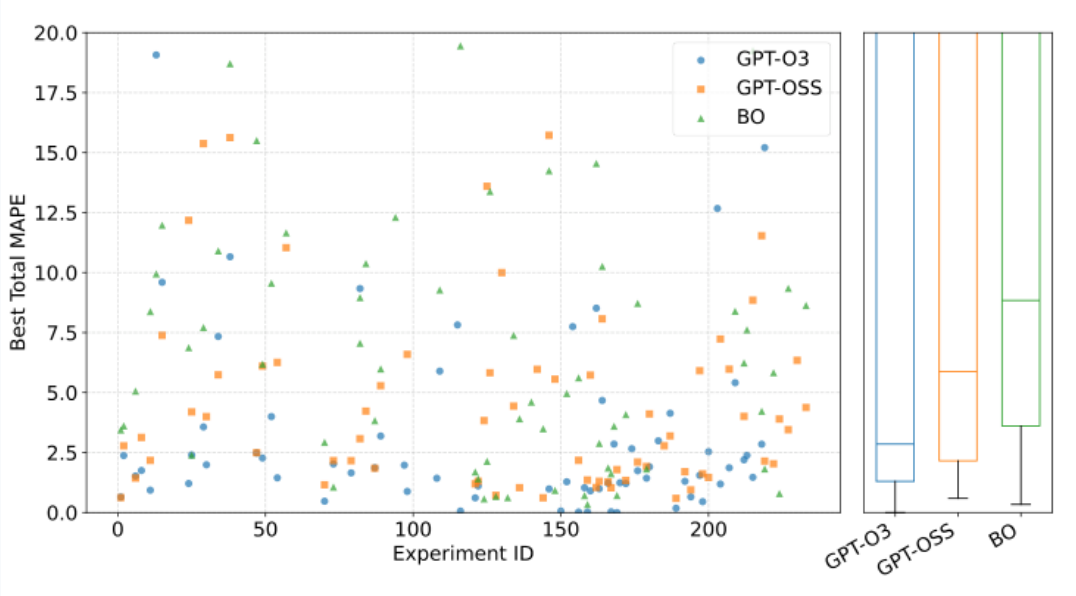
200 个任务：多参数扰动 100 个 + 单参数大幅扰动 100 个

工况：0.2C / 1C / 2C；筛除仿真失败及容量变化小于 1% 的目标。
真实电芯部分使用论文中的公开数据另行验证。

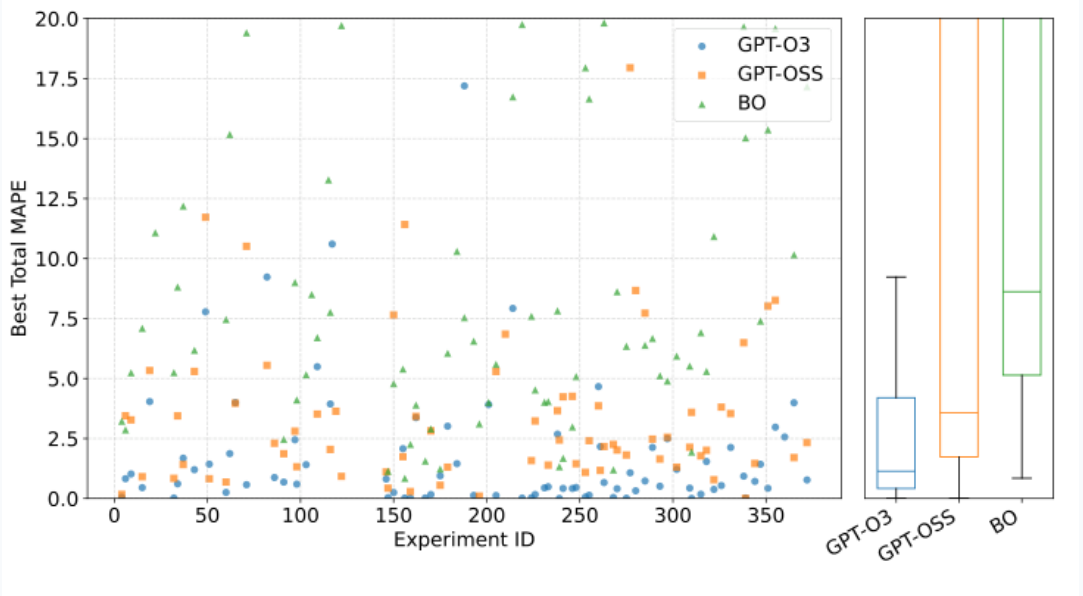
首循环标定：论文原图中的逐任务误差分布

每个点对应一个合成标定任务；右侧箱线图汇总各方法的误差分布。

多参数组合扰动



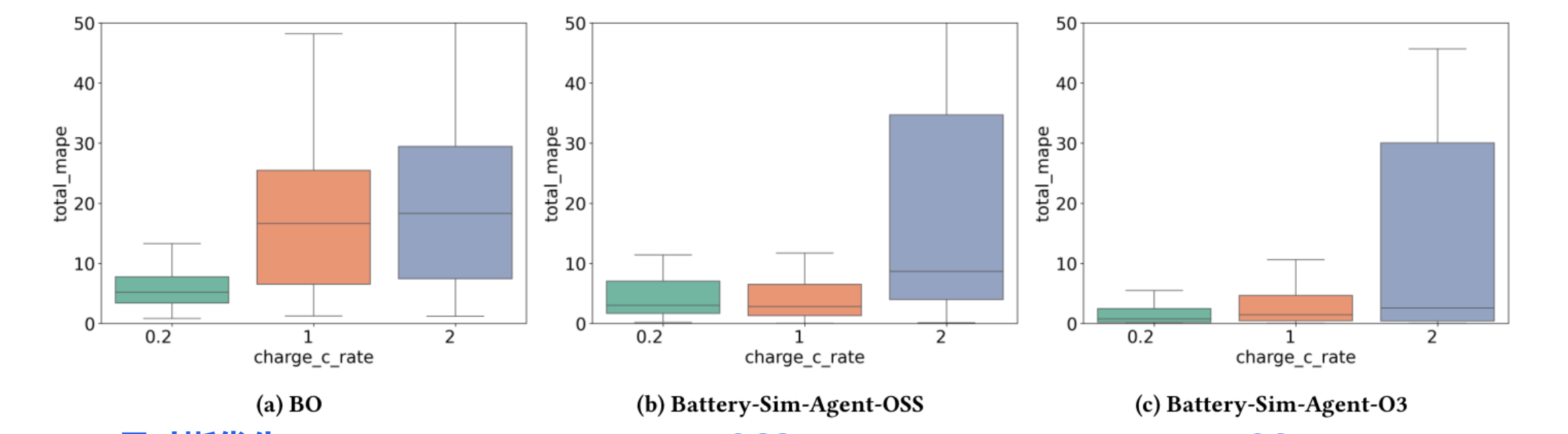
单参数大幅扰动



多参数设定中 Agent-O3 的整体误差更低；单参数大幅扰动下，各方法的优势随任务变化。

不同倍率下的误差分布

在 0.2C、1C、2C 工况中比较三种方法，观察高倍率条件下的标定表现。



贝叶斯优化 **Agent-OSS** **Agent-O3**

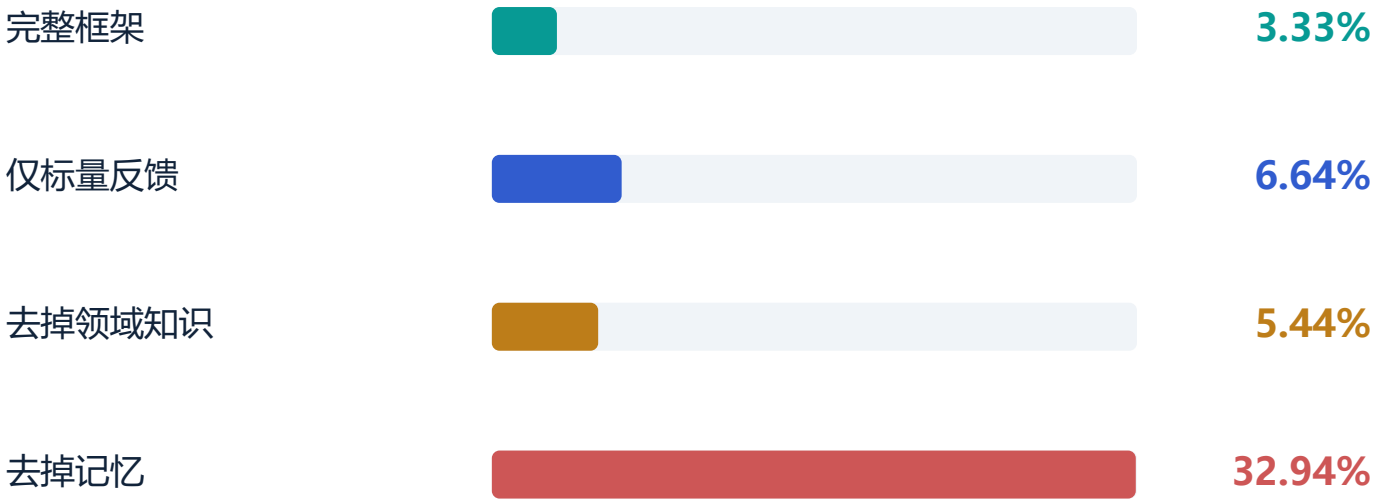
倍率升高会放大动力学与传质差异；Agent-O3 在图示工况中保持较低的误差分布。

Battery-Sim-Agent · Figure 3（论文第 8 页原图裁剪）

框架贡献与计算代价：消融及匹配预算实验

固定主干与统一任务预算，区分框架贡献、基模能力与实际运行开销。

固定 Qwen2.5-32B • 8 个 Chen2020 案例



20 次外循环 • Chen2020

322.4 s

智能体总运行时间

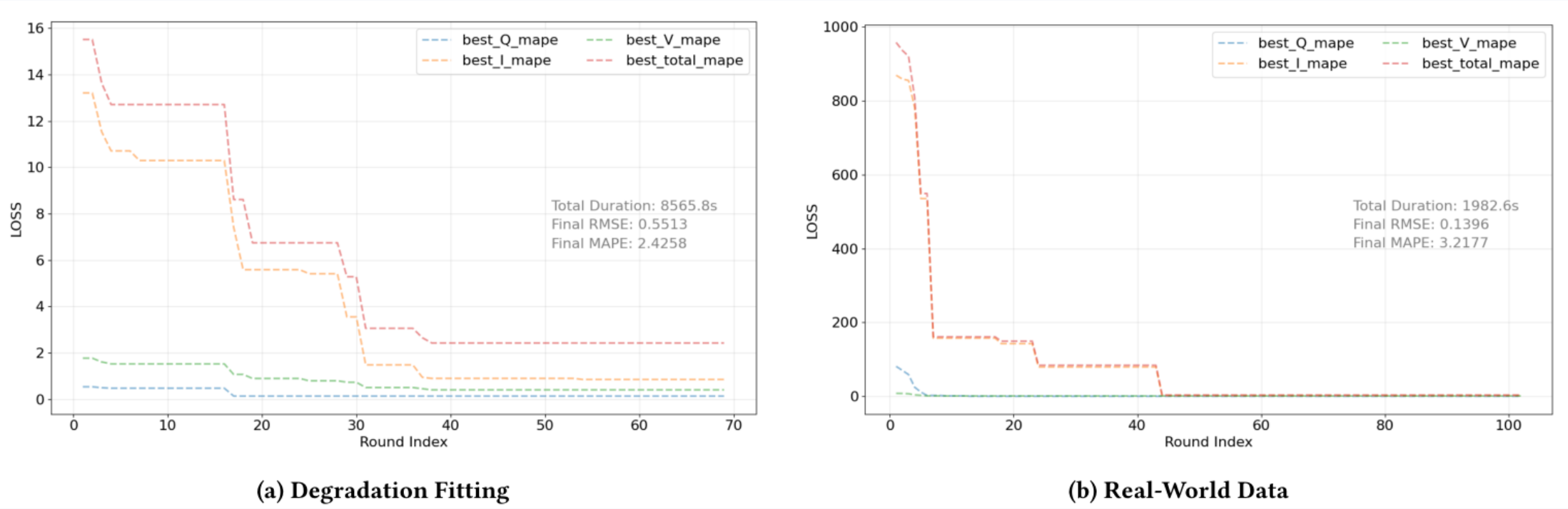
贝叶斯优化总运行时间

541.0 s

Chen2020 单案例 · 相同 20 轮预算

长期退化与真实电芯：原始收敛曲线

左：长期退化参数拟合；右：公开真实电芯数据标定。



长期退化：200 个循环

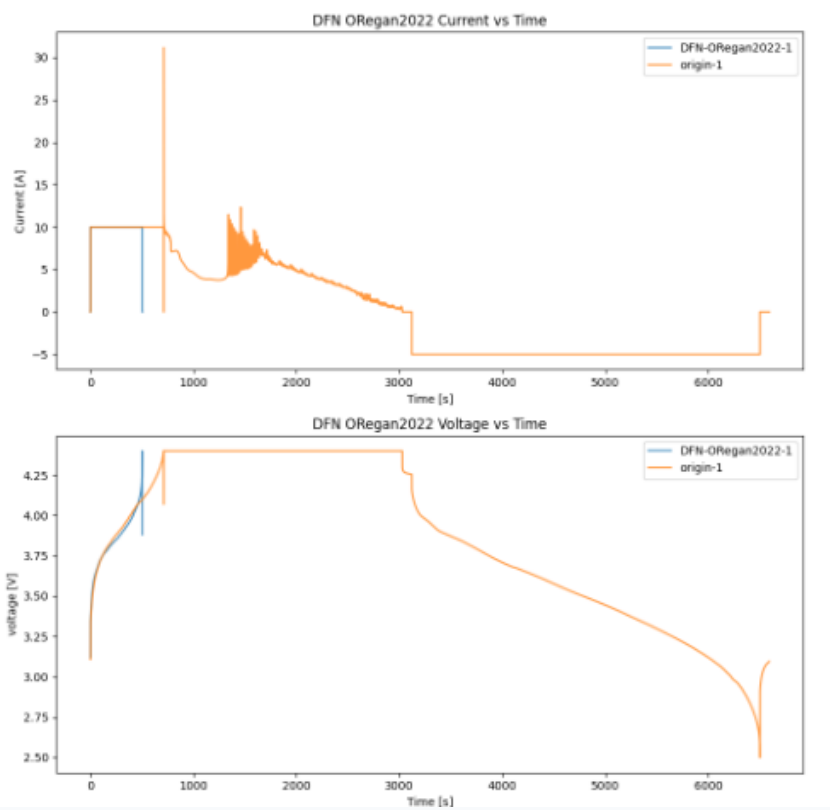
总 MAPE：OSS 1.37% / O3 1.77%

真实电芯：7 个公开数据任务

总 MAPE：OSS 8.75% / O3 3.46%

失败案例：仿真失稳会切断有效反馈

ORegan2022 · 2C 充电 / 1C 放电；初始参数在目标工况下难以稳定求解。



仿真失稳 → 缺少有效反馈

初始仿真约 600 s 提前终止

最初 20 次探索仅 1 次成功

后续仅有 2 次仿真成功

O3 与 BO 也未能有效推进

下一步需要联合处理：可行域搜索、失败归因，以及求解器与优化器的选择。

Battery-Sim-Agent · Appendix D.9 / Figs. 7–8

从参数搜索到仿真与代理模型的协同优化

下一步将参数搜索、仿真校验与代理模型更新组织为联合优化过程。

参数可辨识性

相似曲线可能对应不同参数；需要多协议与先验约束。

数值求解稳定性

高倍率 2C 案例出现仿真大量失败、反馈不足。

优化器选择

根据任务结构与反馈质量，选择合适的优化器。

下一步：物理计算双循环

智能体 / 科研调度
诊断、假设、搜索与预算

高保真仿真器
可信但昂贵的物理反馈

自适应代理模型
主动采样、局部更新、不确定性

研究问题：如何联合决定探索方向、仿真调用与代理模型更新?

从电池参数标定到科学与工程逆问题

给定目标行为，利用仿真与实验反馈寻找满足约束的参数、结构或策略。

正向问题 (θ, u) → 物理仿真 / 实验 → $y = F(\theta, u)$

共同的数学接口，不同的科学任务

标定

参数反演

观测 y^* → 估计 θ^*

设计

逆向设计

目标性能 → 结构 / 配方

控制

约束优化

目标与安全约束 → 策略

按任务的参数结构、仿真成本和反馈质量，选择求解方法。

双循环：参数搜索与代理模型更新

外循环搜索满足目标的方案，内循环通过新样本持续改进代理模型。



当前逆问题驱动新样本采集、局部模型更新与高保真校验。

双循环 RSI: new example

Genoria

EnzymeRSI

Dual loop · Recursive self-improvement

EnzymeRSI:
A dual-loop recursive self-improvement system for enzyme design

Genoria AI Team
Yuejie Hou, Lixiang Yang, Yisi Liu, Weiting Tang, Yueyuxiao Yang, Meng Yang*
Genoria AI, Shenzhen 518083, China

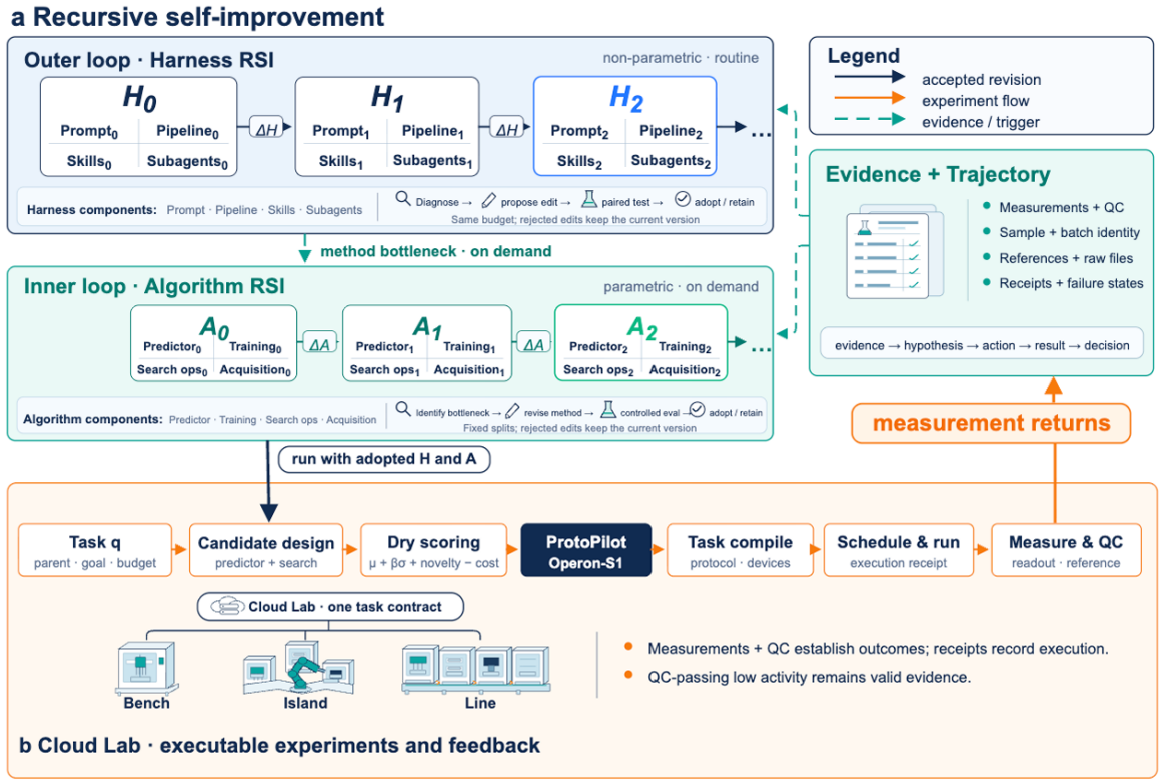
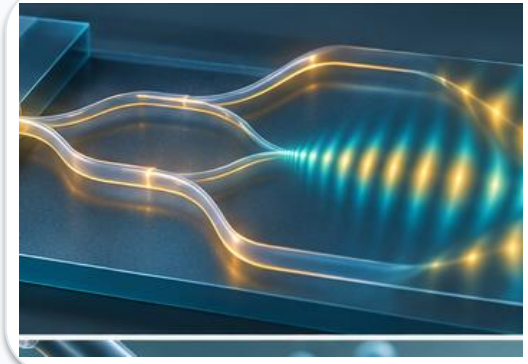


Fig. 1 | The dual-loop structure of EnzymeRSI. a, Dual-loop recursive self-improvement. The outer loop evolves versions of prompts, pipelines, skills and subagents, which are adopted or rolled back after diagnosis, a minimal consistent change bundle and a paired comparison at matched budget; model weights are not modified. The inner loop is triggered only when a method bottleneck appears, and develops predictors, training strategies, search operators and acquisition functions under controlled conditions. Missing packages and permission problems are handled as engineering faults and trigger neither loop. Adoption rules are fixed before the comparison as global adoption, scoped retention or rollback, and an adopted version must be loaded by the next run. The protein, algorithm and system tiers

跨领域拓展：光学、制药、材料与核聚变

各领域都涉及难以直接测量的参数、有限实验预算，以及带物理约束的逆向目标。



量子 / 光子学

几何或介质参数 → 光谱 / 场分布

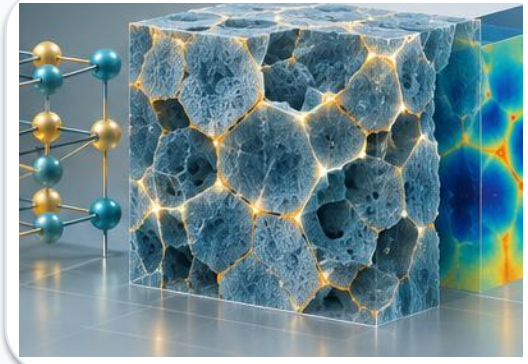
可探索：逆向光学器件设计



制药 / 配方

组分 / 工艺 → 稳定性与功能

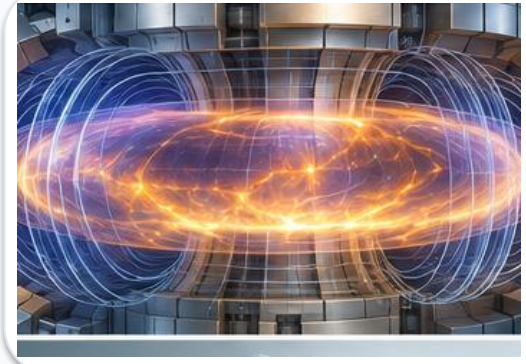
可探索：反向配方与实验设计



材料 / 微结构

成分与结构 → 宏观性能

可探索：多保真材料设计



核聚变 / 等离子体

控制参数 → 等离子体响应

可探索：昂贵仿真与标定

延伸方向：卫星标定与规划 · 数字孪生自动构建 · 科学逆问题

谢谢！期待交流

方樾楷 | 浙江大学

邮箱：fsk@zju.edu.cn
微信：xuangu1996