

# 20230920 斯坦福虚拟小镇

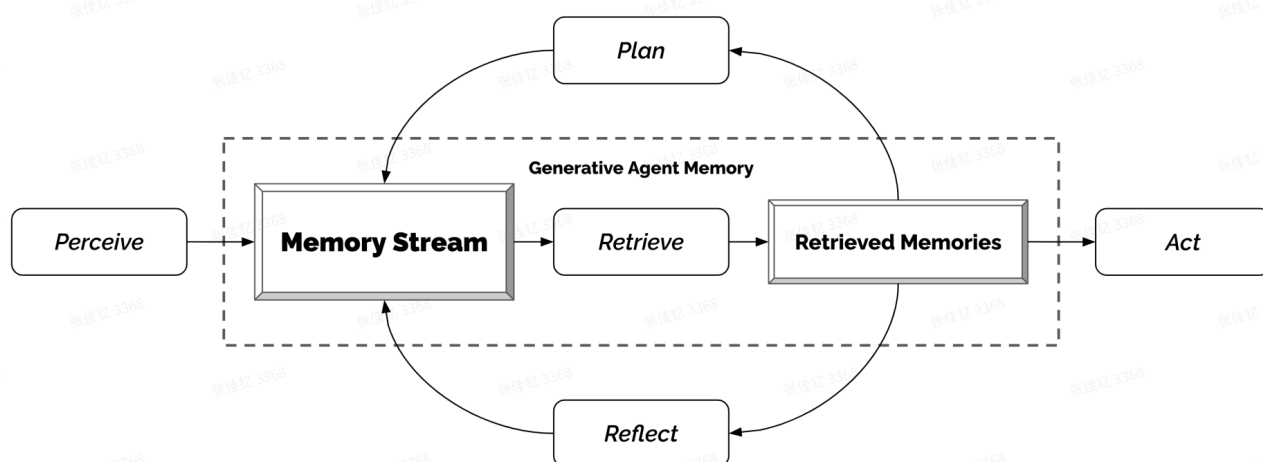
## 介绍

arxiv: [Generative Agents: Interactive Simulacra of Human Behavior](#)

Repo: [https://github.com/joonspk-research/generative\\_agents](https://github.com/joonspk-research/generative_agents)

## 目标

25 个智能体。终端用户可以观察并与之交互，干预他们的日程、分享新闻、建立关系和协调小组活动。最终**用户或开发人员**希望城镇举办游戏内的情人节派对，传统的游戏环境将需要手动编写数十个角色的行为脚本。对于生成智能体，只需告诉**一个智能体**她想举办一场派对就足够了。



智能体感知环境，感知保存在全面记录智能体经历的记忆流中。基于感知，检索相关记忆并使用检索到的动作来确定新动作。检索到的记忆被用于形成长期计划和创建更高层次的反思，这两者又被送入记忆流中被使用。

## 论文贡献


- 可信的人类行为的模拟，动态地受制于智能体不断变化的经验和环境
- 提出一种架构，使生成智能体能够记住、检索、反映、与其他智能体交互，并通过动态变化的环境进行规划。
- 两种评估，架构的重要组成部分以及识别因记忆检索引起的故障
- 讨论互动系统中生成智能体的机会和伦理及社会风险。

## 问题

- 智能体怎么被初始化
- 智能体间由什么触发开始对话？？ Emergent Social Behaviors。对话内容的形式怎样的。如何结束对话。
- MG如何对接沙盒环境，需要增加什么功能
- LLM 在该场景里提示词如何构建
  - 第三人称表达；描述智能体观察、记忆、问题，让LLM进行回答。

## 产品

### 术语

- Time step 时间步。类似沙盒环境中的每一次执行。
  - 在每个时间步里，智能体输出描述当前动作的自然语言表达，比如 `xxx 正在检查邮箱`
- Action 动作。与MG的Action区分，此处为GA 沙盒环境界面上显示的一组表情符号，从上层提供了对动作的抽象表示。
  - 上述时间步里的**自然语言表达会映射成沙盒世界里的具体动作，并通过表情得以表达。**
  - 比如 `检查邮箱` 对应表情 
- 
- 观察
- 规划
- 反思

### 组件

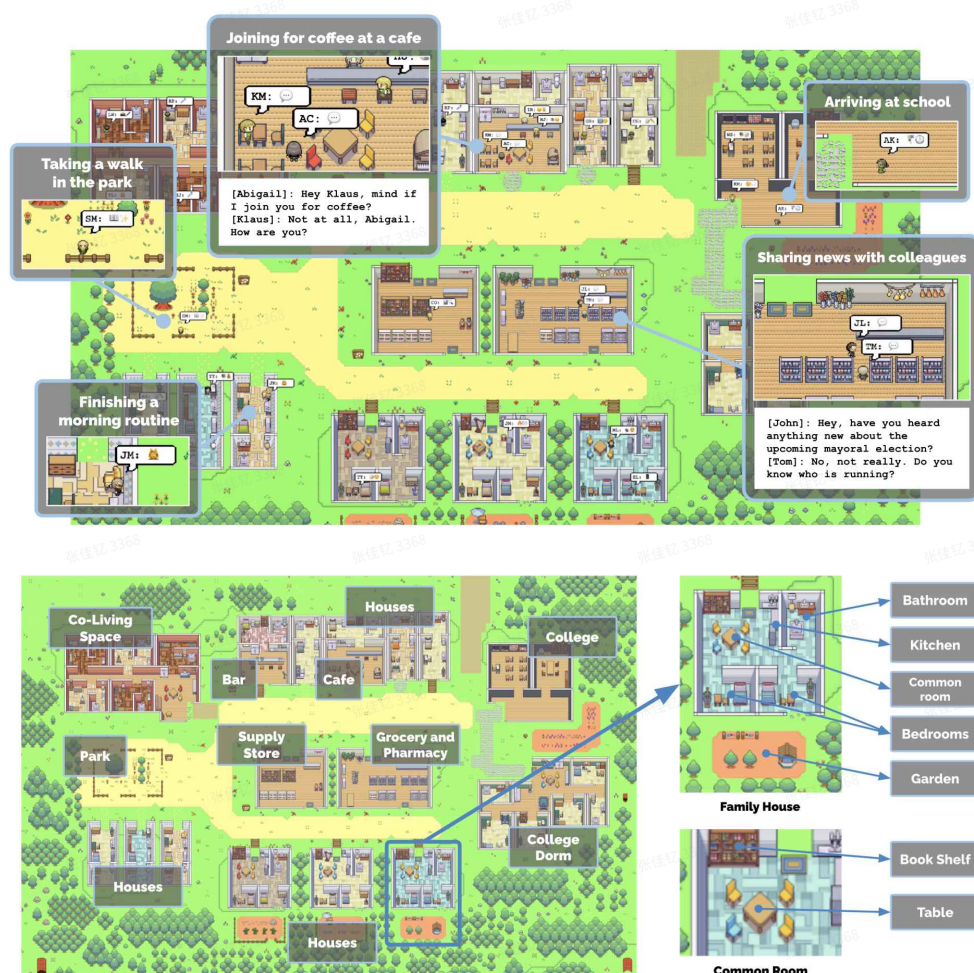
- 记忆流（memory stream）。这是一个长期记忆模块，以自然语言记录智能体经历的完整列表。记忆检索模型结合了相关性、新近度和重要性，以显示通知智能体即时行为所需的记录。
  - 通过“数据库（本质是内存）”来全面记录智能体的经历
  - **记忆流包含观察、反思、计划**
- 反思（reflection）。随着时间的推移将记忆合成更高层次的推论，使智能体能够得出关于自己和他人的结论，以更好地指导其行为。
- 规划（planning）。将这些结论和当前环境转化为高层行动计划，然后递归地转化为行动和反应的详细行为。这些反思和计划会反馈到记忆流中，以影响智能体未来的行为。

## • 评估

- 控制评估（controlled evaluation）。测试智能体是否能够在孤立的情况下产生可信的个体行为。
- 端到端评估（end-to-end evaluation）。智能体在两天的游戏时间内以开放式方式相互交互，以评估智能体的行为。

## 特性

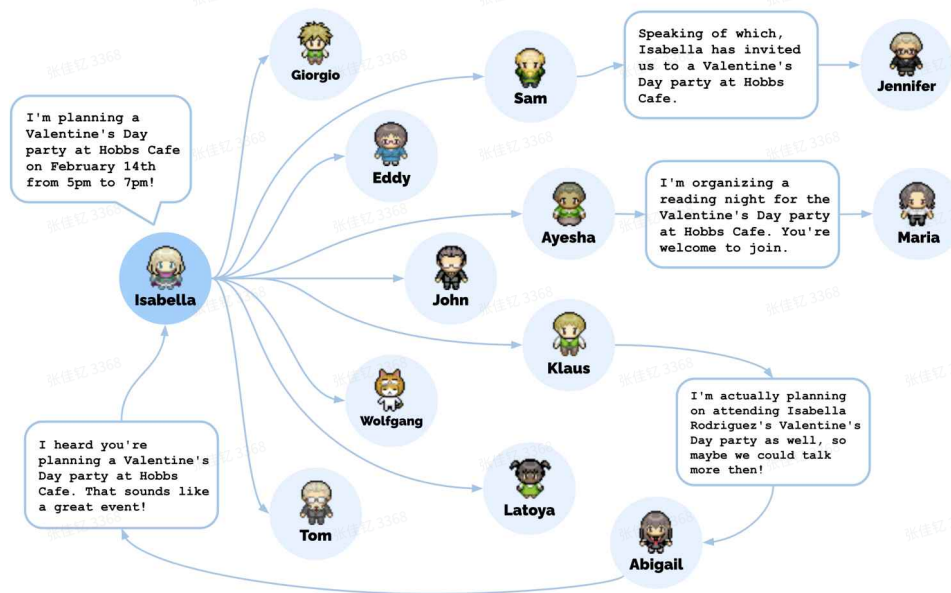
## 产品界面



沙盒环境结构，根节点描述整个世界，房屋、商店等区域为子节点，桌子、书架等为叶子节点。智能体记住的子图为他们所看到的沙盒世界的部分，它能观察到对应部分以及对应的状态。



智能体的一天



举办派对的消息传播

## 实现机制

### 用户

用户指玩或开启虚拟小镇的人，可以通过自然语言与智能体进行对话/通信。

用户可以理解为任意智能体的“分身”，他可以通过自然语言告诉智能体 **将要去做什么事情**，对应的智能体遵循 **指令** 并在后续步中展开对应的行为。

例如：对话中，用户告诉智能体Joan他将在选举中与智能体Sam竞争。Joan将参加选举并于家人分享该信息。

## 生成式智能体

### 智能体

智能体表示

生成式智能体：当前环境和过去的经验作为输入，并生成行为作为输出。

种子记忆：一段自然语言描述来描述智能体的身份，包括它的职业和与其他智能体的关系。每段信息用分号分隔，并在模拟开始时分别作为初始记忆。

智能体描述示例

1 John Lin is a pharmacy shopkeeper at the Willow Market and Pharmacy who loves to help people. He is always looking for ways to make the process of getting medication easier for his customers; John Lin is living with his wife, Mei Lin, who is a college professor, and son, Eddy Lin, who is a student studying music theory;...

智能体通信

通信方式：自然语言内容

能感知其他智能体在他们的本地区域以及生成智能体架构决定他们是否走过或参与对话。

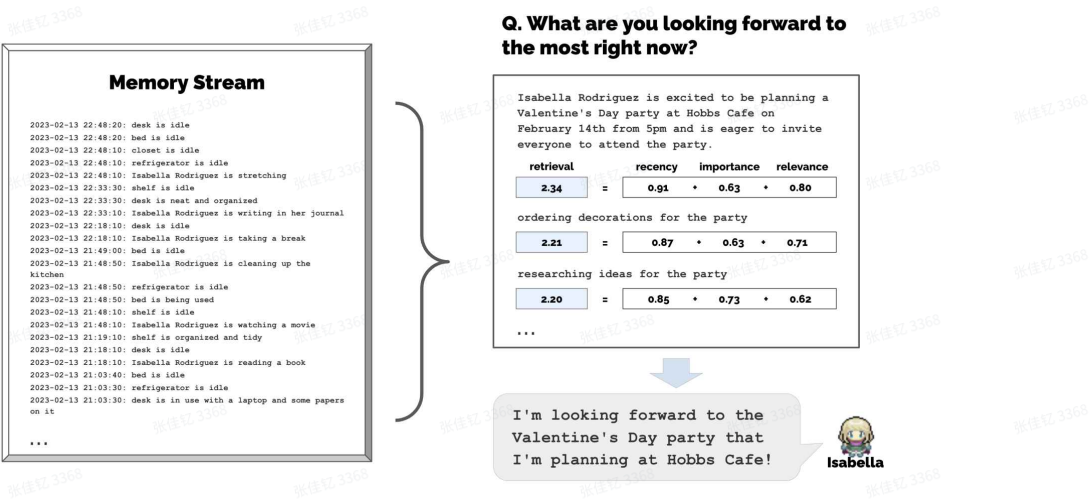
记忆

记忆（记忆流）：内存对象列表

组成：自然语言描述、创建时间戳、访问时间戳

记忆流的最基本元素是观察，观察（感知）到的内容组成了对应的记忆。包括智能体本身执行的行为，也包括感知到的其他智能体或非智能体对象执行的行为或状态（例如：xxx正在在邮件、燃气灶是打开状态）

检索





检索权重

- Recency 。越近访问过的记忆权重越高。将recency作为自上次检索记忆以来沙盒游戏小时数的指数衰减函数，衰减因子 0.995。
- 重要性。直接让LLM对以及做出1-10的评分，越高越重要。
- 相关性。[0-1]范围的embedding检索，余弦相似度作为相关性。

记忆评分：上述三者相加（和=1）

反思

出发点：光有记忆智能体很难做出推论，需要更高层次的思考。

反思也是一种记忆，反思后会加入到记忆中（多种记忆类型）

举例：

Q：智能体A与谁共度一个小时

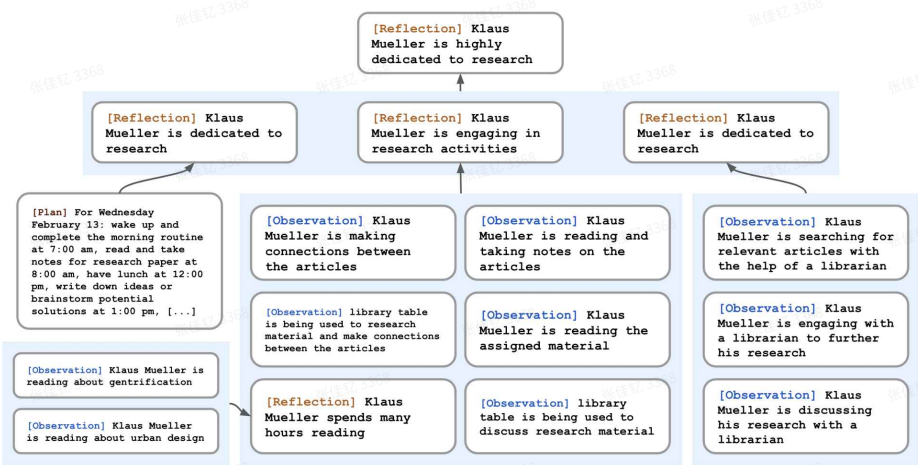
A1：直接得选择接触频繁的人，智能体B虽然是舍友但打交道少。

A2：智能体A从专注科研多天的记忆中得出他热爱研究的高层次反馈。同时智能体C也付出了科研努力，两者更有话题。因此，选择智能体C更格式。

对最近重要性记忆的分数总和超过预设的150时，对最近记忆进行反思。

流程：记忆集合；LLM总结Topk个高级问题；对生成问题进行检索汇总相关记忆；LLM针对问题作出高级见解回应。

智能体可以生成反思树，树的叶节点表示基本观察，而非叶节点表示思想，这些思想在树中越高，就变得越抽象和越高级。



规划

目的：智能体需要在更长的时间范围内进行计划，以确保他们的动作序列是连贯和可信的。

流程：计划（**Plan，也被存储在记忆流中**）描述智能体的未来动作序列，并帮助保持智能体的行为随时间的一致性。计划包括位置、开始时间和持续时间。

实现：计划的制定和动态更新

## 如何制定计划

- 创建初始计划，我们用智能体的摘要描述提示语言模型（例如，姓名、特征和他们最近经历的总结）和他们前一天的总结。此处生成粗略计划。
- 通过**递归**的方式对粗粒度动作进行进一步拆解
- **根据对环境观察**，决定智能体是否应该继续执行其现有计划或做出反应更新。
  - LLM结合智能体观察和对应记忆生成**总结描述**，并提出应该针对观察做出什么反应。根据回答重新更新自己的计划。
    - 智能体总结描述（summary description） - LLM prompt
      - 智能体状态：在做什么
      - 智能体观察：看到什么
      - 智能体记忆总结：对记忆流的总结
      - 是否需要观察做出回应，什么是适当的回应。

## 如何开始对话

- 结合智能体总结记忆和向其他智能体的询问项，进行问题的生成。
  - 通用的，被询问智能体结合自己历史记录和对话历史进行回应。
  - 持续上述过程进行连续对话，直到**任一智能体结束对话**
    - `plan.generate_convo`
      - `converse.agent_chat_v2`（默认最多8轮）
        - 判断是否结束：`iterative_convo_v1.txt`
- 智能体总结描述 - LLM prompt
  - 智能体状态：在做什么
  - 智能体观察：看到什么
  - 智能体记忆总结：对记忆流的总结
  - 打算询问关于xxx的事项，怎么开始提问

智能体John的提示词

- 1 [Agent's Summary Description]
- 2 It is February 13, 2023, 4:56 pm.
- 3 John Lin's **status**: John is back home early from work.
- 4 **Observation**: John saw Eddy taking a short walk around his workplace.
- 5 **Summary of relevant context** from John's memory: Eddy Lin is John's **Lin's son**. Eddy Lin has been working on a music composition for his class. Eddy Lin likes to walk around the garden when he is thinking about or listening to music.
- 6 John is asking Eddy about his music composition project. **What would he say to Eddy?**

智能体John向智能体Eddy提问的问题（通过LLM得到）

- 1 Hey Eddy, how's the music composition project for your class coming along?

智能体Eddy生成回应的提示词

- 1 [Agent's Summary Description]
- 2 It is February 13, 2023, 4:56 pm.
- 3 Eddy Lin's status: Eddy is taking a short walk around his workplace.
- 4 Observation: John is initiating a conversation with Eddy.
- 5 Summary of relevant context from Eddy's memory: John Lin is Eddy Lin's father. J
- 6 Here is the dialogue history:
- 7 John: Hey Eddy, how's the music composition project for your class coming along?
- 8 **How would Eddy respond to John?**

智能体Eddy回复John的内容

- 1 **Hey Dad**, it's going well. I've been taking walks around the garden to clear my h

## 沙盒游戏世界Smallville

### 沙盒环境结构

沙盒环境的区域和对象作为一个树的数据结构，在树中的边缘表示在沙盒世界的包容关系。**将树转换成自然语言传递给生成智能体**。例如，“stove”是“kitchen”的子项，被渲染为“there is a stove in the kitchen”。



## 智能体环境

环境树初始化每个智能体，环境树捕获智能体应该知道的空间和对象（房间、商店等），当智能体在沙盒世界中导航时，它们更新该树以反映新感知的区域。

### 智能体位置确定

遍历智能体存储的环境树，并将其一部分扁平化为自然语言以提示语言模型。递归地从智能体环境树的根开始，我们提示模型找到最合适的区域。

- 1 [Agent's Summary Description]
- 2 Eddy Lin is currently in The Lin family's house: Eddy Lin's bedroom: desk) that has Mei and John Lin's bedroom, Eddy Lin's bedroom, common room, kitchen, bathroom, and garden.
- 3 Eddy Lin knows of the following areas: The Lin family's house, Johnson Park, Harvey Oak Supply Store, The Willows Market and Pharmacy, Hobbs Cafe, The Rose and Crown Pub.
- 4 \* Prefer to stay in the current area if the activity can be done there.
- 5 Eddy Lin is planning to take a short walk around his workspace.
- 6 Which area should Eddy Lin go to?

当一个智能体对一个对象执行一个动作时，我们提示语言模型询问对象的状态发生了什么。

## 沙盒环境实现

Smallville沙盒游戏环境是使用Phaser网页游戏开发框架构建。并在基础上，搭建了后端服务对接沙盒环境信息和智能体。

环境基础：智能体生活空间都有统一的设施配套。

### 后端服务数据结构

沙箱世界中每个智能体的信息

- 它们的当前位置
- 它们当前动作的描述
- 它们正在与之交互的沙箱对象

### 每个沙盒时间步

- 沙盒服务器解析JSON以获得来自生成智能体的任何改变，将智能体移动到它们的新位置，并且更新生成智能体的任何沙盒对象的状态。
- 将每个智能体的预设可视范围内的所有智能体和对象发送到该智能体的存储器，以便智能体可以适当地做出反应。智能体的动作输出更新JSON。

## 沙盒环境交互

智能体移动：由生成智能体框架和沙盒Smallville指导。模型指示智能体到某一位置，计算智能体到达路径，智能体进行移动。

用户可进入沙盒环境中进而控制具体的智能体，智能体被不被控制并不受影响。但**用户可以向环境对象发出更改状态**（比如煤气炉由打开改为燃烧，对应智能体会在下一时刻关掉炉子继续做早餐。）

## 评估

### 控制评估

### 评估什么

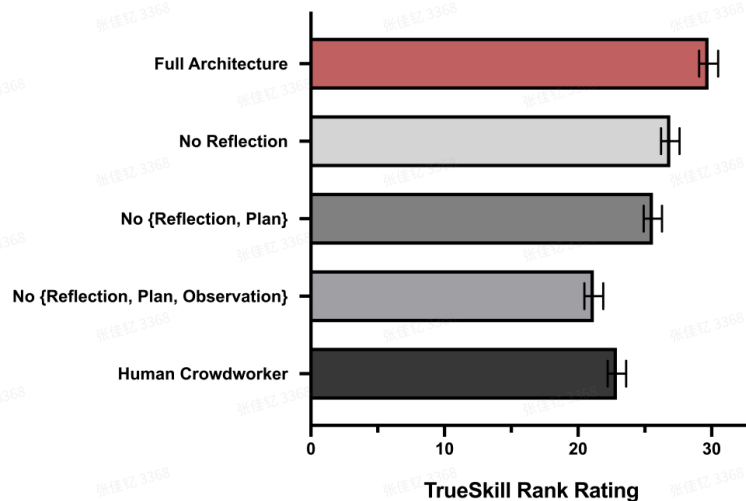
- 个体智能体是否正确地检索过去的经验，并产生可信的计划、反应。
- 智能体表现出信息扩散，关系的形成，并进行协调

### 怎么评估

- 对问题回答的检索
  - 五个问题类别（保持自我认知，检索记忆，制定计划，反应和反思），每个类别，提出五个问题（**论文附录有完整列表**）。
- 自我认知
  - 例如：大致描述您的典型工作日安排
- 检索记忆
  - 特定事件人物，例如 **XX是谁**
- 计划
  - 检索长期计划，例如 **明天上午10点安排**
- 反应
  - 针对假设情况，智能体需要可信的响应，例如 **你的早餐烧糊了！你会怎么做？**
- 反思
  - 智能体利用他们通过更高层次的推理获得的对他人和自己的更深入的理解。例如 **有一小时的共处时间，你会选择谁**

### 评估消融

- 无观察、无反思、无计划架构，而不访问存储器流中的任何内容，诸如观察、计划和反思
- 无反思、无计划架构，其具有对存储器流中的观察的访问，但不具有对计划或反思的访问
- 无反思体系结构，其可以访问观察和计划，但不可以访问反思。



招募了100名评估员针对上述5种情况产生了100组排名数据，采用ELO国际象棋评分系统中的TrueSkill评级进行。给定一组排名结果，TrueSkill输出每个情况的平均评级值和标准差。

## 端到端评估

针对观察到的智能体的突发社会行为的可信度进行评估。

## 突发社会行为

指对应的行为非预定义的，通过智能体间的信息相互交互，形成新的关系以及协同行动。

- 信息传播
  - 智能体注意到彼此，则开始对话并交换各自知道的信息。并且信息可能随着对话变多逐渐传播。
- 关系记忆
  - 随着时间步演进，智能体会形成新的关系并记住与其他智能体的互动。即结实了新的智能体。
- 协调
  - 智能体间的相互协调。从单智能体的初始意图设定（举办派对），在传播、协作（装饰派对）、预约、参加派对等相互作用的社会行为。

## 怎么评估

- 信息传播
  - 示例：通过设定智能体A将举办派对，一定周期后看其他智能体对该事情的了解度。
  - 验证：通过被问智能体记忆流中对应信息所涉及的历史对话来验证回答是否真实
- 关系记忆
  - 验证：通过问智能体双方是否互相认识，都得到确认回复则证明形成关系。
- 协调

验证：确认出席派对的人数

## 代码

```
1 |— environment
2 |   |— frontend_server # 带界面的
3 |       |— compressed_storage # 用于回放
4 |           |— July1_the_ville_isabella_maria_klaus-step-3-20
5 |               |— master_movement.json
6 |               |— meta.json
7 |               |— personas
8 |       |— frontend_server
9 |           |— settings # Django
10 |           |— urls.py # 沙盒界面
11 |       |— global_methods.py # 无用。3
12 |       |— manage.py # Django
13 |       |— static_dirs
14 |           |— assets
15 |               |— characters # 智能体
16 |               |— the_ville # 沙盒环境
17 |       |— storage # 沙盒仿真
18 |           |— July1_the_ville_isabella_maria_klaus-step-3-1 # 单次仿真
19 |               |— environment
20 |               |— movement
21 |               |— personas
22 |               |— reverie
23 |       |— temp_storage
24 |       |— templates # 前端html
25 |       |— translator
26 |       |— migrations # 库表更新
27 |       |— views.py # 与 frontend_server 交互
28 |— reverie
29 |   |— backend_server
30 |       |— maze.py # 地图 (
31 |       |— path_finder.py # 地图上
32 |       |— persona # 智能体
33 |           |— cognitive_modules # 感知模块
34 |               |— converse.py # 对话,
35 |               |— execute.py # 智能体
36 |               |— perceive.py # 感知,
37 |               |— plan.py # 计划,
38 |               |— reflect.py # 反思,
39 |               |— retrieve.py # 记忆检索
40 |       |— memory_structures
```

41				— associative_memory.py	# 关联记
42				— scratch.py	# 短期记
43				— spatial_memory.py	# 空间记
44				— persona.py	# 智能体
45				— prompt_template	
46				— <del>defunct_run_gpt_prompt.py</del>	# 未实际
47				— gpt_structure.py	# 提示词
48				— print_prompt.py	
49				— run_gpt_prompt.py	# 智能体
50				— v1	# 提示词
51				— reverie.py	# 后端沙
52				— utils.py	# 后端服
53				— compress_sim_storage.py	
54				— global_methods.py	

## 存在问题

1. 最常见的错误：智能体未能检索相关记忆、对智能体记忆进行捏造修饰（幻觉）或从语言模型继承过于正式的言语或行为
2. 不稳定行为模式
  - a. 记忆积累越多，检索最相关信息和选择执行动作的恰当地理位置上变得有挑战
    - i. 比如：吃饭，跑去了酒馆。
  - b. 正确行为的错误分类，一些容易产生歧义的自然语言词汇被记忆
    - i. 比如：宿舍浴室一般一个人用，但会出现多人同时进入。可以通过强调为 单人浴室解决。
  - c. 指令似乎引导智能体的行为变得更加礼貌和正式。
    - i. 随着长上下文加入，LLM会回复些与智能体设定不符的回答（不喜欢的兴趣变得喜欢等）
3. 模拟成本高
  - a. 25个智能体需要多天花费几千美元（gpt-3.5-turbo）完成

## 参考