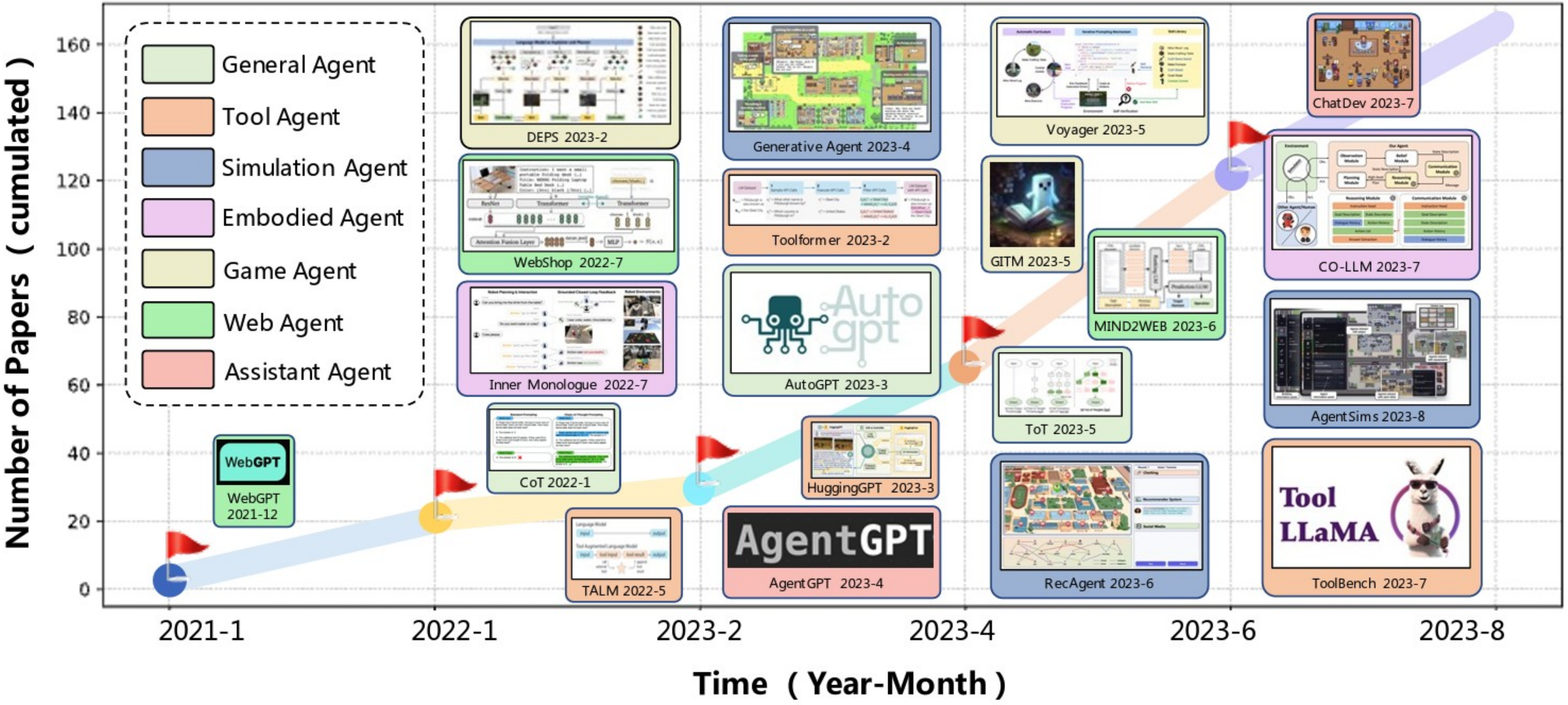
Agentic AI

LLM-based Autonomous Agents

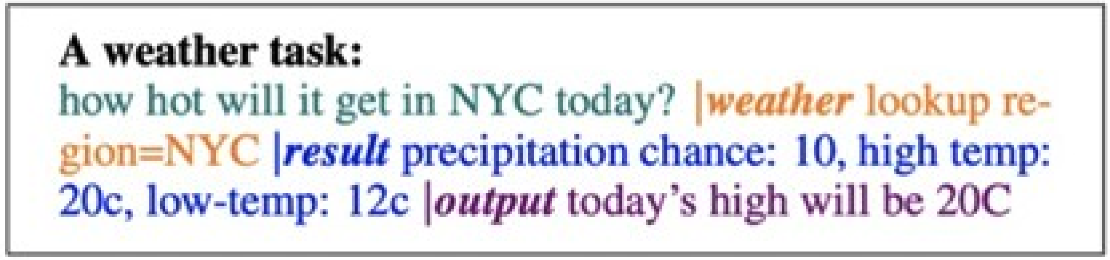


Agent

- An “intelligent” system that interacts with some “environment”
- Basic recipe (current)
  - LLM
  - Tool
  - Memory (past thoughts and actions, etc)
  - Knowledge & reasoning
  - human

Tool

- Special tokens to invoke tool calls for
    - Search engine, calculator, etc.
    - Task-specific models (e.g., translatio
    - APIs

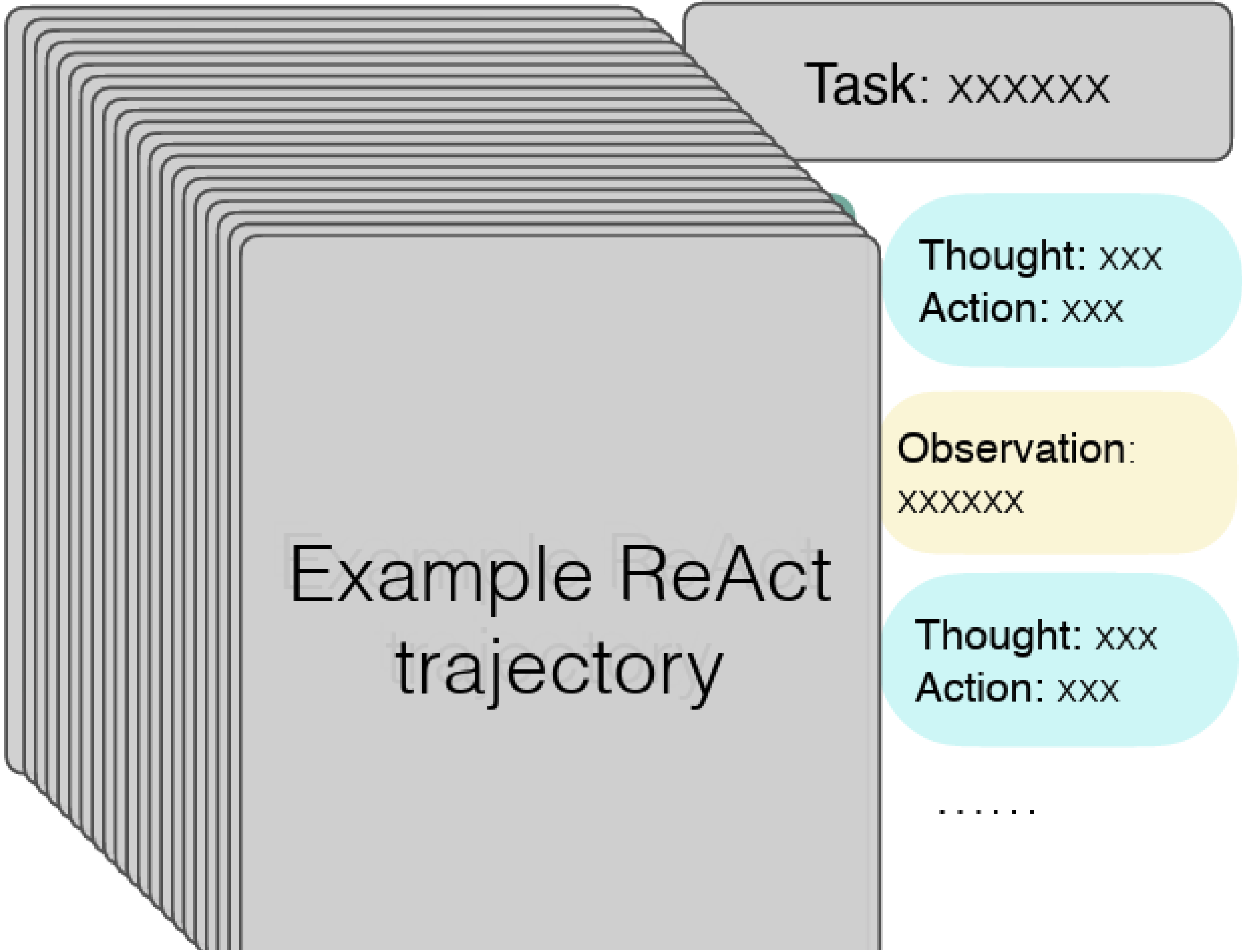


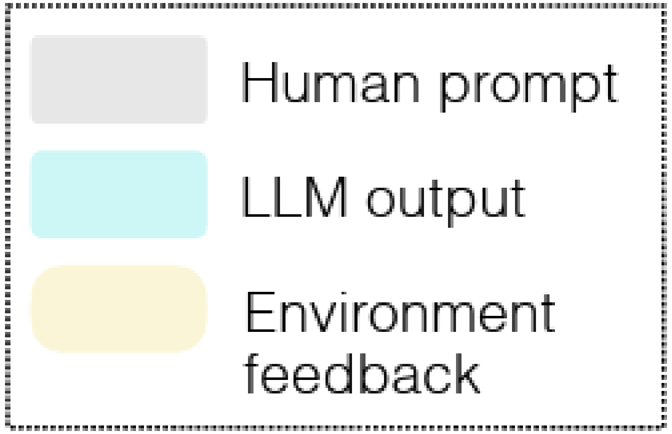
A weather task:
how hot will it get in NYC today? |*weather* lookup region=NYC |*result* precipitation chance: 10, high temp: 20c, low-temp: 12c |*output* today's high will be 20C

TALM: Tool Augmented Language Models.

Recap: ReAct

- ReAct supports
  - One-shot promptin
  - Few-shot promptin
  - Fine-tuning





A zero-shot ReAct prompt

You are an agent that answers questions by using two actions:

- search[query]: Google search the query. You can also use it to calculate math.
- finish[answer]: return the answer

Your generation should have the following format:

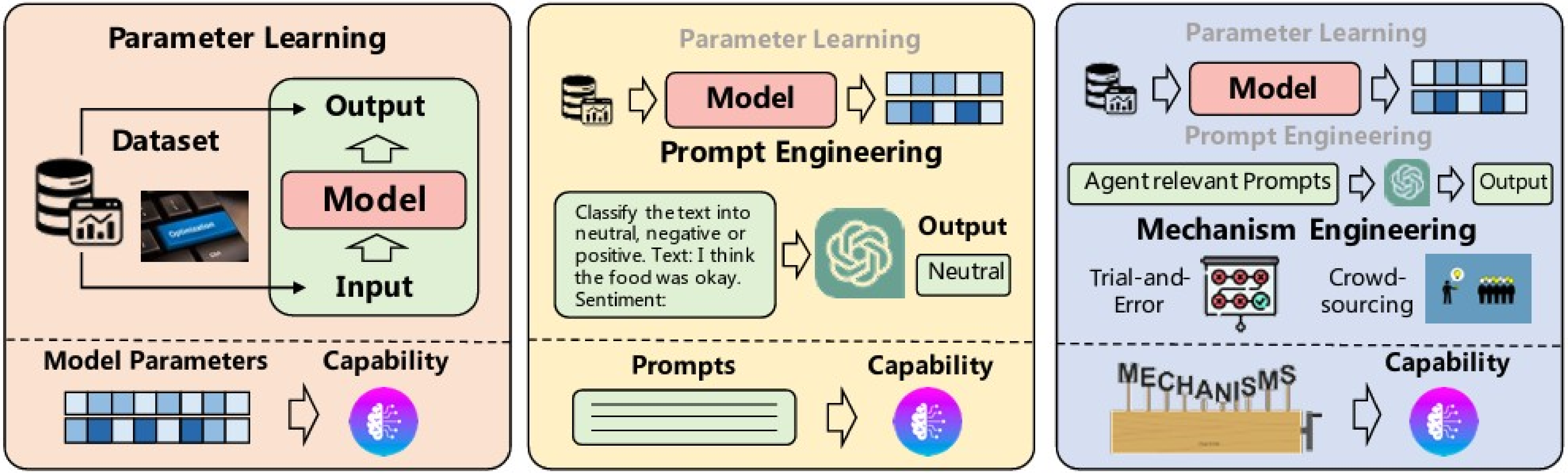
Thought: to analyze the observation and inform the action.

Action: your action

Question: If I have seven trillion dollars today, can I buy Apple, Nvidia, and Microsoft? If not, how much more money do I need?

Mechanism design

Lei Wang et al. A Survey on Large Language Model based Autonomous Agents



The era of machine learning

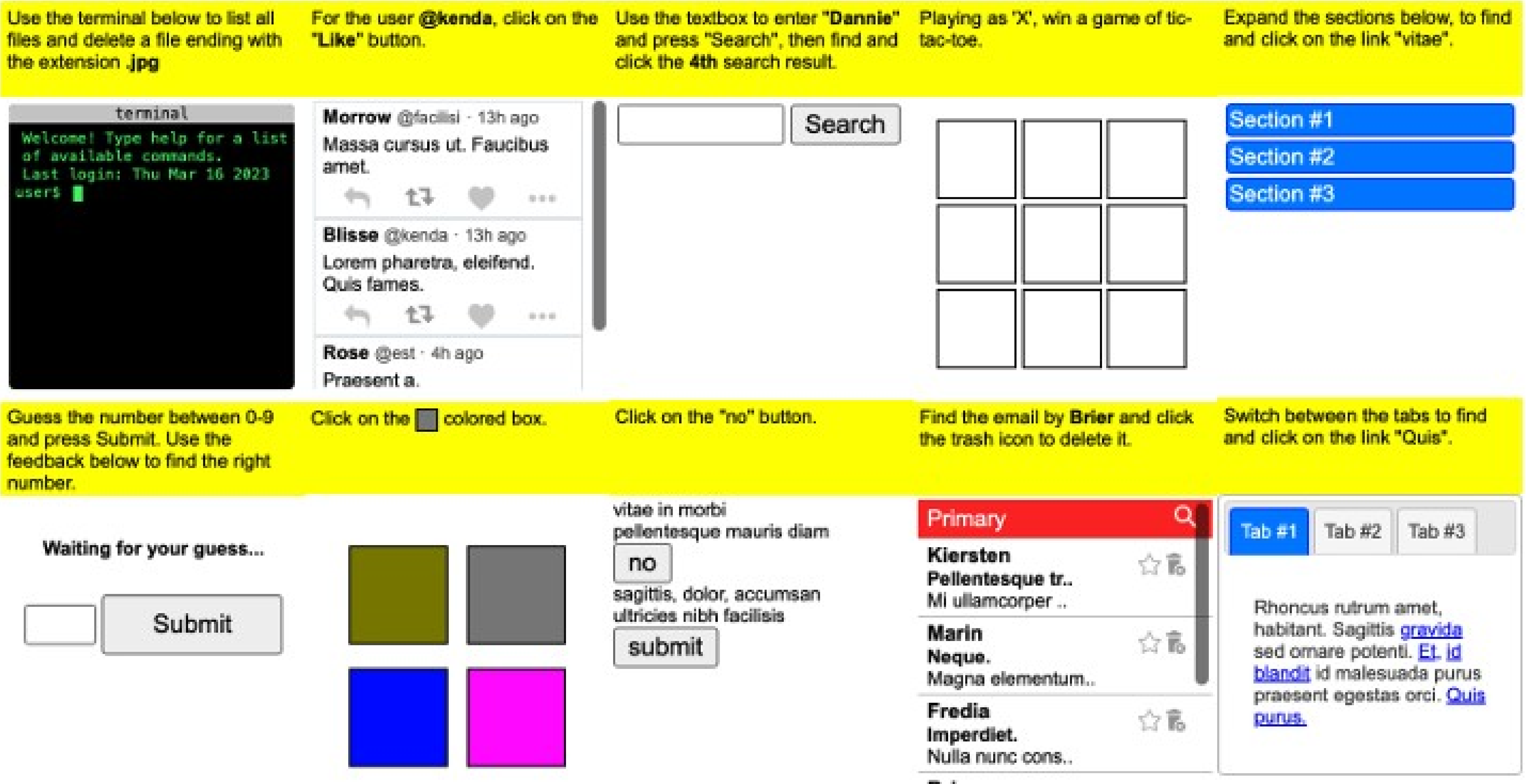
The era of large language model

The era of agent

Agents in Practice

- Single Agent
  - Task-oriented
  - Innovation-oriented
  - Lifecycle-oriented
- Multi-agent
  - Cooperative
  - Adversarial
- Human-agent interaction

Language Models can Solve Computer Tasks (NeurIPS'23)



Use the terminal below to list all files and delete a file ending with the extension .jpg

```
terminal
Welcome! Type help for a list
of available commands.
Last login: Thu Mar 16 2023
user$ █
```

For the user **@kenda**, click on the "**Like**" button.

Morrow @facilisi · 13h ago
Massa cursus ut. Faucibus amet.

Blisse @kenda · 13h ago
Lorem pharetra, eleifend. Quis fames.

Rose @est · 4h ago
Praesent a.

Use the textbox to enter "**Dannie**" and press "Search", then find and click the **4th** search result.

Playing as 'X', win a game of tic-tac-toe.

Expand the sections below, to find and click on the link "vitae".

Guess the number between 0-9 and press Submit. Use the feedback below to find the right number.

Waiting for your guess...

Click on the ▨ colored box.

Click on the "no" button.

vitae in morbi pellentesque mauris diam

sagittis, dolor, accumsan ultricies nibh facilisis

Find the email by **Brier** and click the trash icon to delete it.

Kiersten
Pellentesque tr..
Mi ullamcorper ..

Marin
Neque.
Magna elementum..

Fredia
Imperdiet.
Nulla nunc cons..

Switch between the tabs to find and click on the link "Quis".

Rhoncus rutrum amet, habitant. Sagittis gravida sed ornare potenti. Et id blandit id malesuada purus praesent egestas orci. Quis purus.

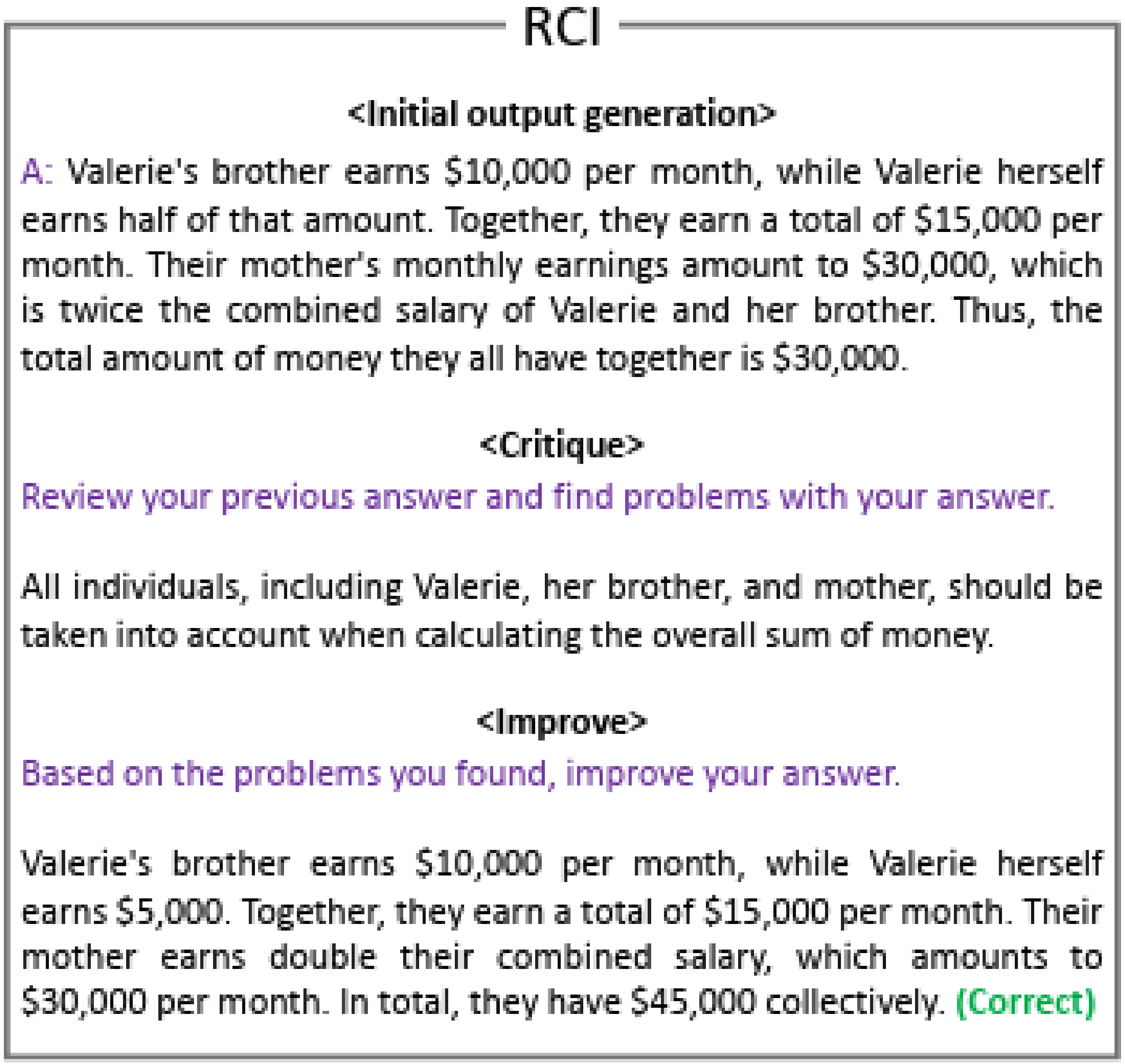
Agent uses keyboard strokes and mouse clicks to accomplish the task.

Every task contains a natural language prompt in yellow.

RCI Prompting

- Recursively Criticizes and Improves

- Used in three reasoning steps
  - Task grounding
  - State grounding
  - Agent grounding



RCI

<Initial output generation>

A: Valerie's brother earns $10,000 per month, while Valerie herself earns half of that amount. Together, they earn a total of $15,000 per month. Their mother's monthly earnings amount to $30,000, which is twice the combined salary of Valerie and her brother. Thus, the total amount of money they all have together is $30,000.

<Critique>

Review your previous answer and find problems with your answer.

All individuals, including Valerie, her brother, and mother, should be taken into account when calculating the overall sum of money.

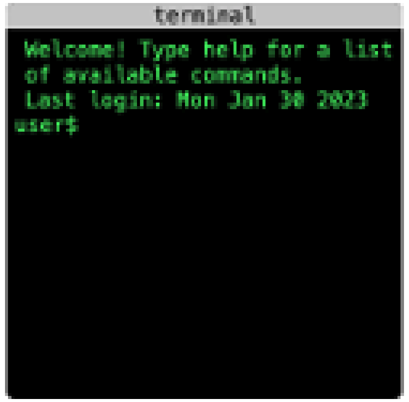
<Improve>

Based on the problems you found, improve your answer.

Valerie's brother earns $10,000 per month, while Valerie herself earns $5,000. Together, they earn a total of $15,000 per month. Their mother earns double their combined salary, which amounts to $30,000 per month. In total, they have $45,000 collectively. (Correct)

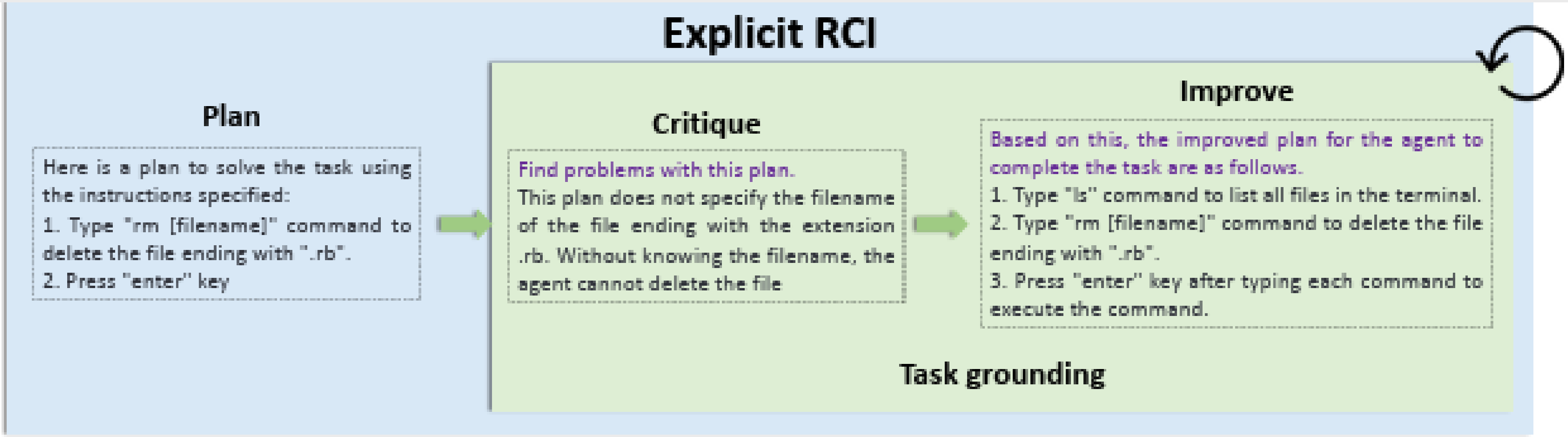
Grounding

- Task grounding
  - Generating a plan of actionable steps
  - Actions are sampled, considering the present state, task and generated plan
- State grounding
  - Enhance the task-grounded actions to be feasible in the current state
  - Implicit RCI
- Agent grounding
  - guarantee the admissibility of actions derived from the language model
  - consider specifications of the computer agent
  - Implicit RCI



```
Welcome! Type help for a list
 of available commands.
 Last login: Mon Jan 30 2023
user$
```

Initial state



Explicit RCI

Plan

Here is a plan to solve the task using the instructions specified:
1. Type "rm [filename]" command to delete the file ending with ".rb".
2. Press "enter" key

Critique

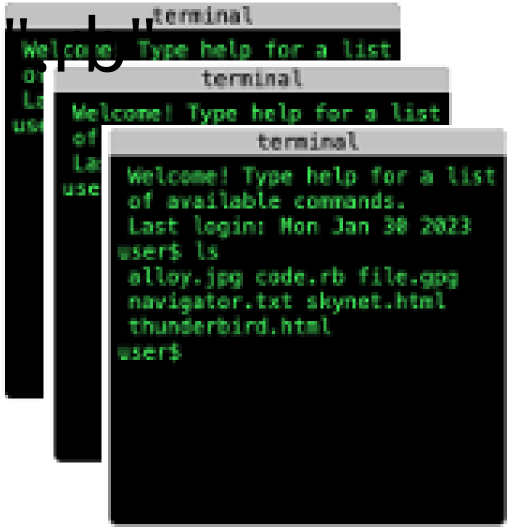
Find problems with this plan.
This plan does not specify the filename of the file ending with the extension .rb. Without knowing the filename, the agent cannot delete the file

Improve

Based on this, the improved plan for the agent to complete the task are as follows.
1. Type "ls" command to list all files in the terminal.
2. Type "rm [filename]" command to delete the file ending with ".rb".
3. Press "enter" key after typing each command to execute the command.

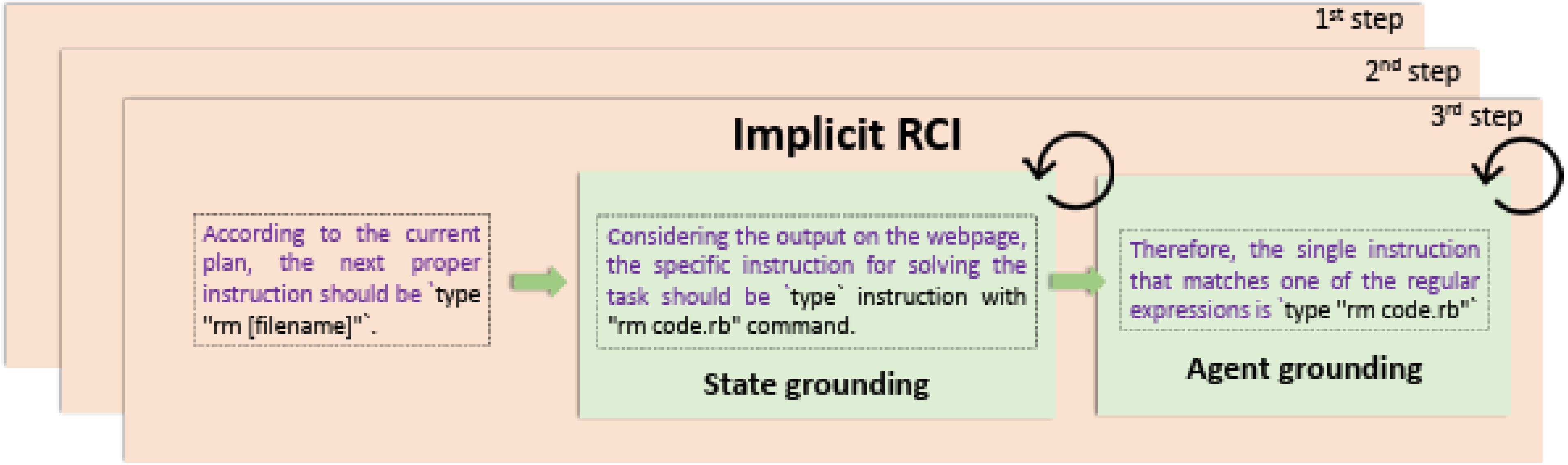
Task grounding

Task: using the terminal to delete a file ending with ".rb"



```
Welcome! Type help for a list
 of available commands.
 Last login: Mon Jan 30 2023
user$ ls
 alloy.jpg code.rb file.gpg
 navigator.txt skynet.html
 thunderbird.html
user$
```

Current state



Implicit RCI

According to the current plan, the next proper instruction should be `type "rm [filename]"`.

Considering the output on the webpage, the specific instruction for solving the task should be `type` instruction with "rm code.rb" command.

State grounding

Therefore, the single instruction that matches one of the regular expressions is `type "rm code.rb"`

Agent grounding

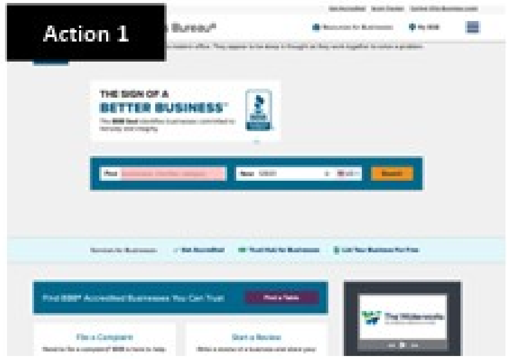
- prompts are in purple, remaining text shows the output of LLM
- Final step: executed by the instruction-following agent on the environment

MIND2WEB: Towards a Generalist Agent for the Web (NeurIPS’23)

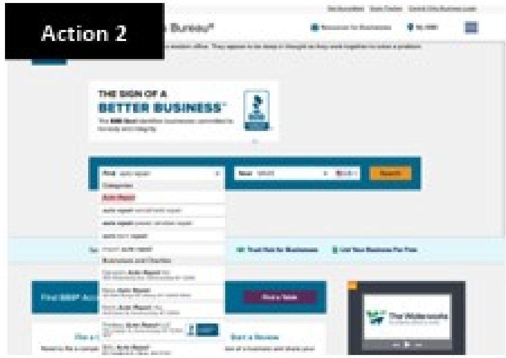
Task Description: Show me the reviews for the auto repair business closest to 10002

Action Sequence:

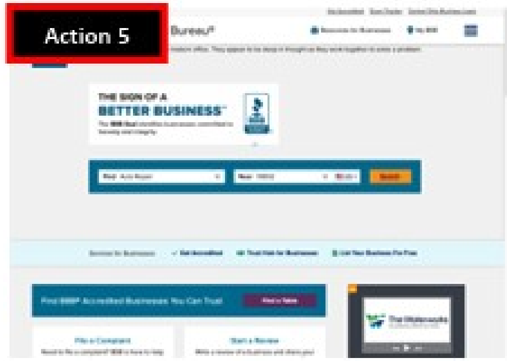
	Target Element	Operation
1.	[searchbox] *Find*	TYPE: *auto repair*
2.	[button] *Auto Repair*	CLICK
3.	[textbox] *Near*	TYPE: *10002*
4.	[button] *10002*	CLICK
5.	**[button] *Search***	**CLICK**
6.	[switch] *Show BBB Accredited only*	CLICK
7.	[svg]	CLICK
8.	[button] *Sort By*	CLICK
9.	**[link] *Fast Lane 24 Hour Auto Repair***	**CLICK**
10.	[link] *Read Reviews*	CLICK



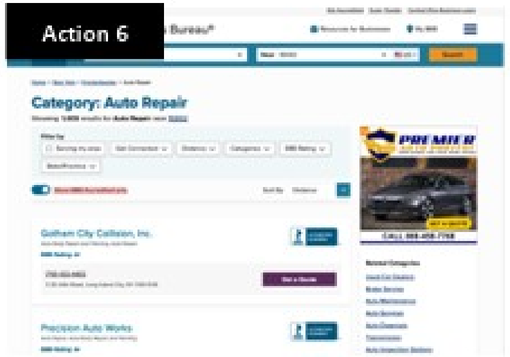
`<input name="find_text" type="search">`



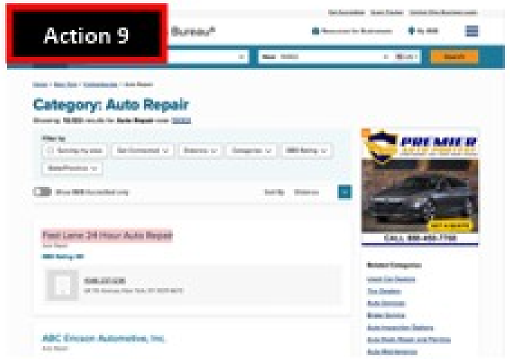
`<em>Auto Repair</em>`



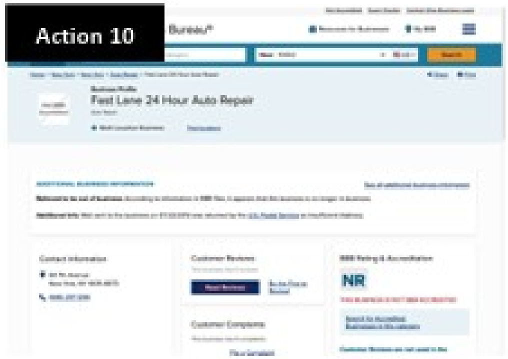
`<button>Search</button>`



`<button>Show BBB Accredited only</button>`



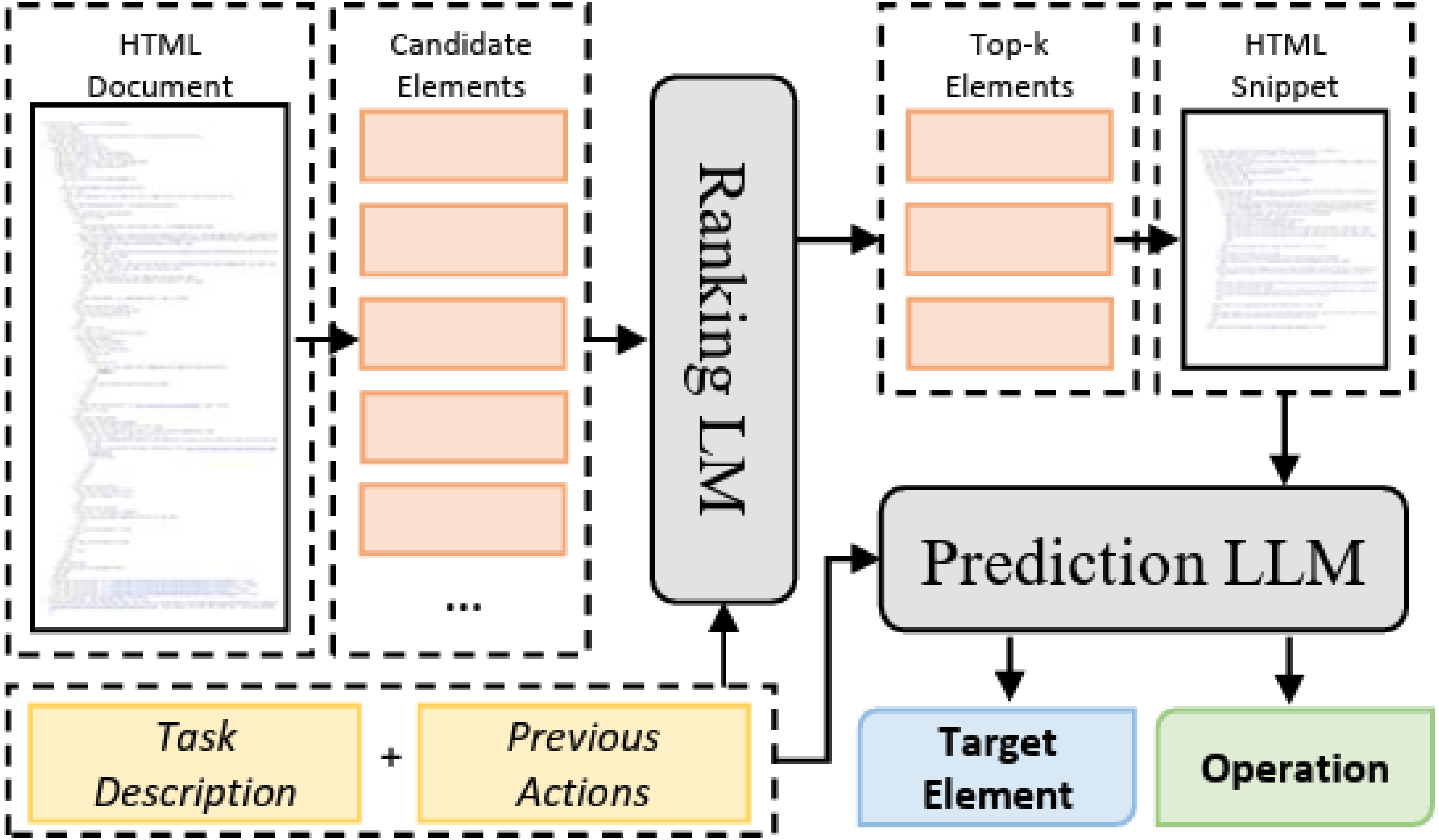
`<span>Fast Lane 24 Hour Auto Repair</span>`



`<a href="link:XXX">Read Reviews</a>`

Actions marked in red will result in a transition to a new webpage

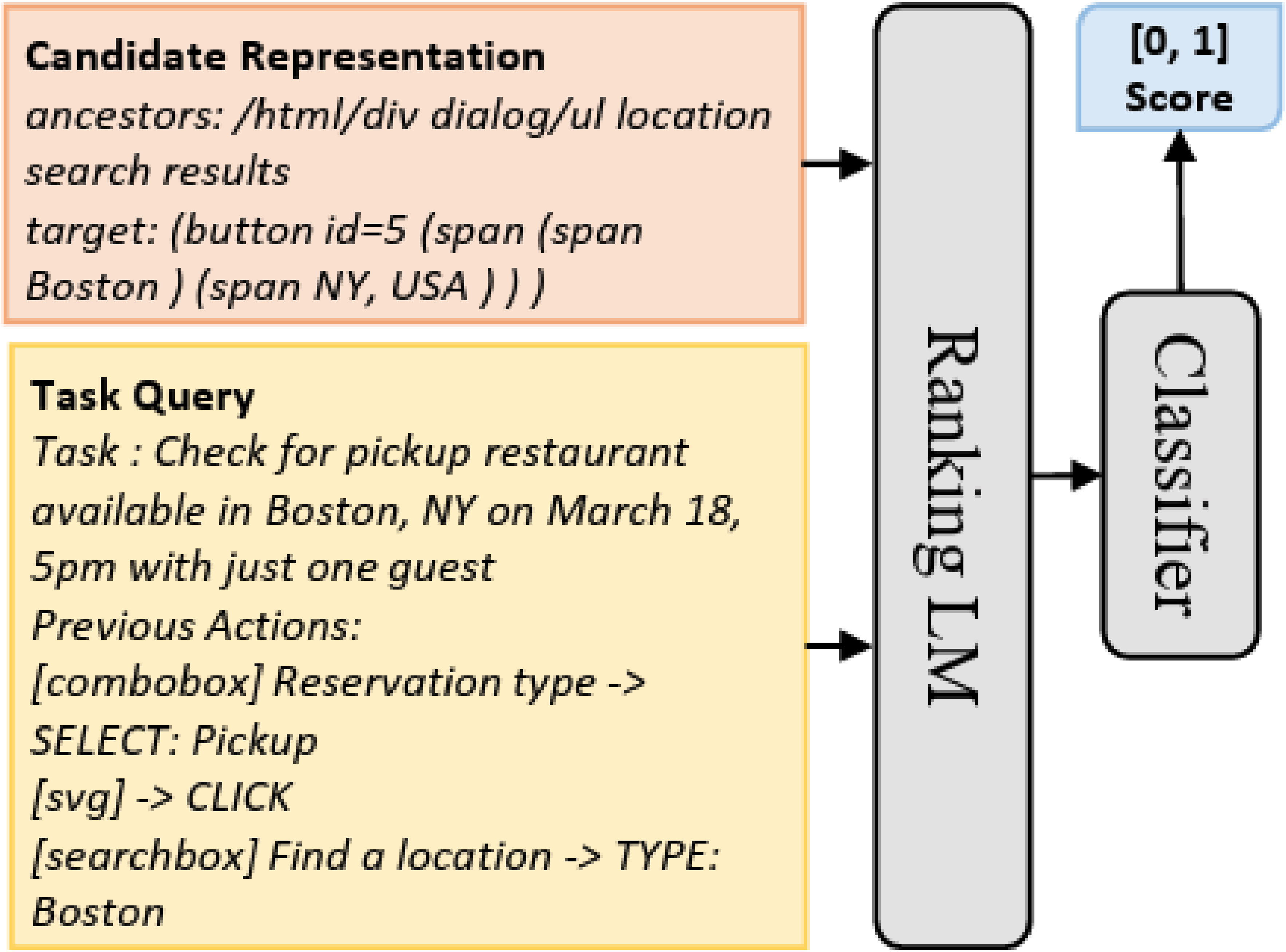
MINDACT



- two-stage process
- Candidate generation with small LMs
- Action prediction with LLMs

Candidate generation

- Rank the DOM elements present on a webpage
- Cross encoder



Candidate Representation

ancestors: /html/div dialog/ul location search results

target: (button id=5 (span (span Boston) (span NY, USA)))

Task Query

Task : Check for pickup restaurant available in Boston, NY on March 18, 5pm with just one guest

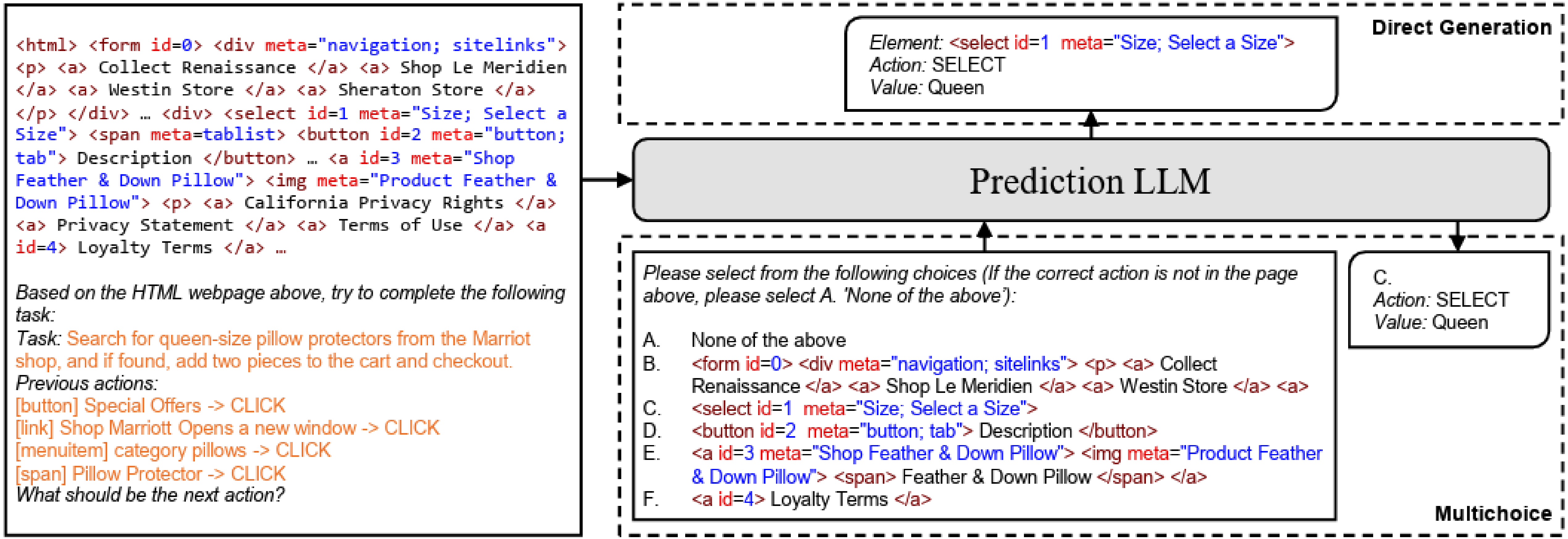
Previous Actions:

[combobox] Reservation type -> SELECT: Pickup

[svg] -> CLICK

[searchbox] Find a location -> TYPE: Boston

Action prediction



```
<html> <form id=0> <div meta="navigation; sitelinks">
<p> <a> Collect Renaissance </a> <a> Shop Le Meridien
</a> <a> Westin Store </a> <a> Sheraton Store </a>
</p> </div> … <div> <select id=1 meta="Size; Select a
Size"> <span meta=tablist> <button id=2 meta="button;
tab"> Description </button> … <a id=3 meta="Shop
Feather & Down Pillow"> <img meta="Product Feather &
Down Pillow"> <p> <a> California Privacy Rights </a>
<a> Privacy Statement </a> <a> Terms of Use </a> <a
id=4> Loyalty Terms </a> …
```

Based on the HTML webpage above, try to complete the following task:
Task: Search for queen-size pillow protectors from the Marriot shop, and if found, add two pieces to the cart and checkout.
Previous actions:
[button] Special Offers -> CLICK
[link] Shop Marriott Opens a new window -> CLICK
[menuitem] category pillows -> CLICK
[span] Pillow Protector -> CLICK
What should be the next action?

Prediction LLM

Direct Generation

Element: <select id=1 meta="Size; Select a Size">
Action: SELECT
Value: Queen

Multichoice

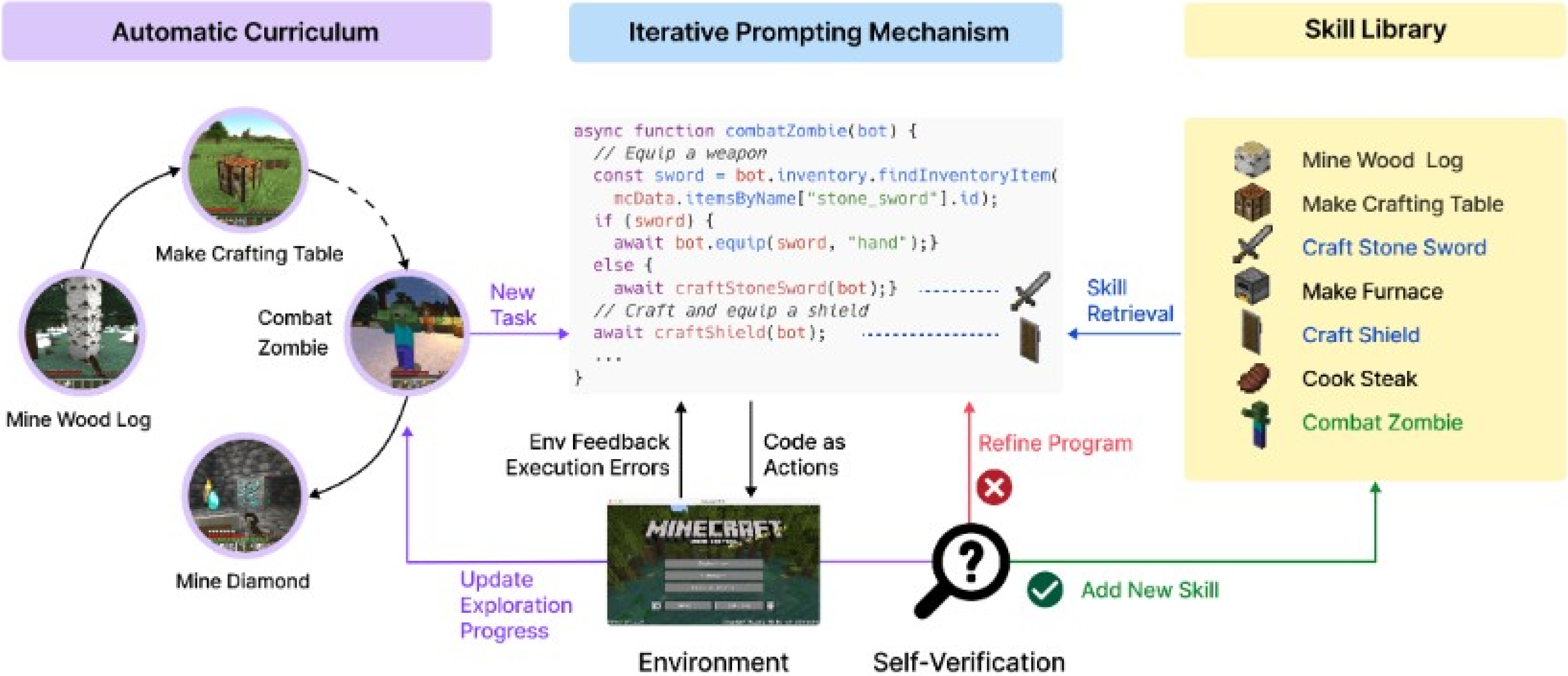
Please select from the following choices (If the correct action is not in the page above, please select A. 'None of the above'):

A. None of the above
B. <form id=0> <div meta="navigation; sitelinks"> <p> <a> Collect Renaissance </a> <a> Shop Le Meridien </a> <a> Westin Store </a> <a>
C. <select id=1 meta="Size; Select a Size">
D. <button id=2 meta="button; tab"> Description </button>
E. <a id=3 meta="Shop Feather & Down Pillow"> <img meta="Product Feather & Down Pillow"> <span> Feather & Down Pillow </span> </a>
F. <a id=4> Loyalty Terms </a>

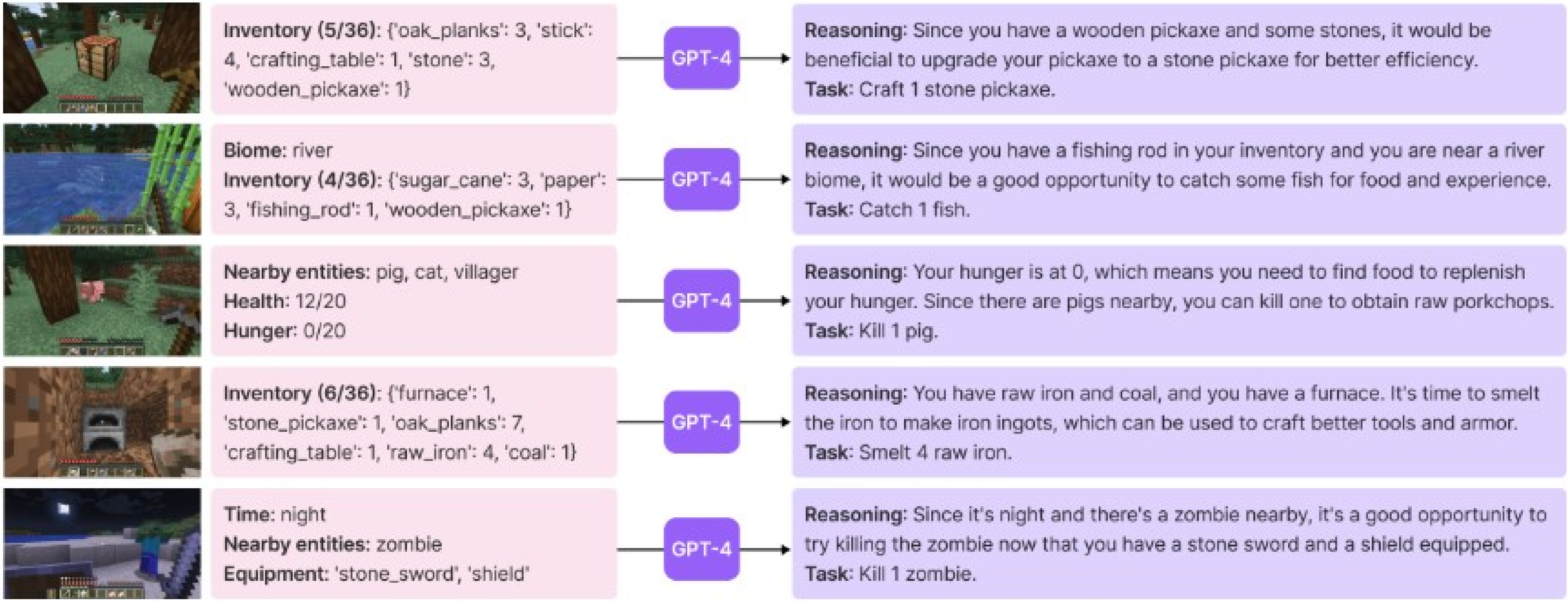
C.
Action: SELECT
Value: Queen

- MCQ works better than direct generation

Voyager: An Open-Ended Embodied Agent with Large Language Models (ICLR’25)



```
async function combatZombie(bot) {
  // Equip a weapon
  const sword = bot.inventory.findInventoryItem(
    mcData.itemsByName["stone_sword"].id);
  if (sword) {
    await bot.equip(sword, "hand");}
  else {
    await craftStoneSword(bot);}
  // Craft and equip a shield
  await craftShield(bot);
  ...
}
```



Inventory (5/36): {'oak_planks': 3, 'stick': 4, 'crafting_table': 1, 'stone': 3, 'wooden_pickaxe': 1}

Reasoning: Since you have a wooden pickaxe and some stones, it would be beneficial to upgrade your pickaxe to a stone pickaxe for better efficiency.
Task: Craft 1 stone pickaxe.

Biome: river
Inventory (4/36): {'sugar_cane': 3, 'paper': 3, 'fishing_rod': 1, 'wooden_pickaxe': 1}

Reasoning: Since you have a fishing rod in your inventory and you are near a river biome, it would be a good opportunity to catch some fish for food and experience.
Task: Catch 1 fish.

Nearby entities: pig, cat, villager
Health: 12/20
Hunger: 0/20

Reasoning: Your hunger is at 0, which means you need to find food to replenish your hunger. Since there are pigs nearby, you can kill one to obtain raw porkchops.
Task: Kill 1 pig.

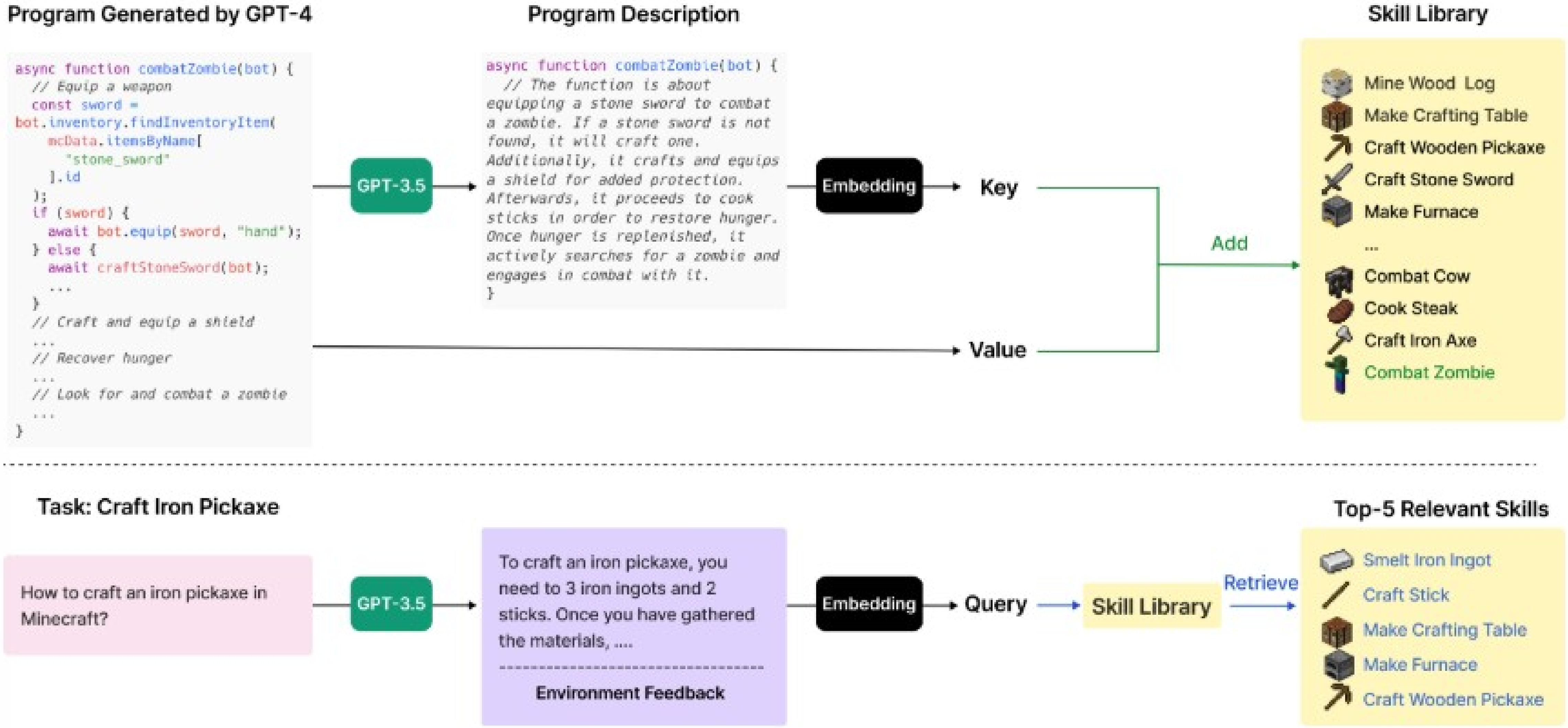
Inventory (6/36): {'furnace': 1, 'stone_pickaxe': 1, 'oak_planks': 7, 'crafting_table': 1, 'raw_iron': 4, 'coal': 1}

Reasoning: You have raw iron and coal, and you have a furnace. It's time to smelt the iron to make iron ingots, which can be used to craft better tools and armor.
Task: Smelt 4 raw iron.

Time: night
Nearby entities: zombie
Equipment: 'stone_sword', 'shield'

Reasoning: Since it's night and there's a zombie nearby, it's a good opportunity to try killing the zombie now that you have a stone sword and a shield equipped.
Task: Kill 1 zombie.

Automatic curriculum. The automatic curriculum takes into account the exploration progress and the agent's state to maximize exploration. The curriculum is generated by GPT-4 based on the overarching goal of "discovering as many diverse things as possible". This approach can be perceived as an in-context form of *novelty search*.



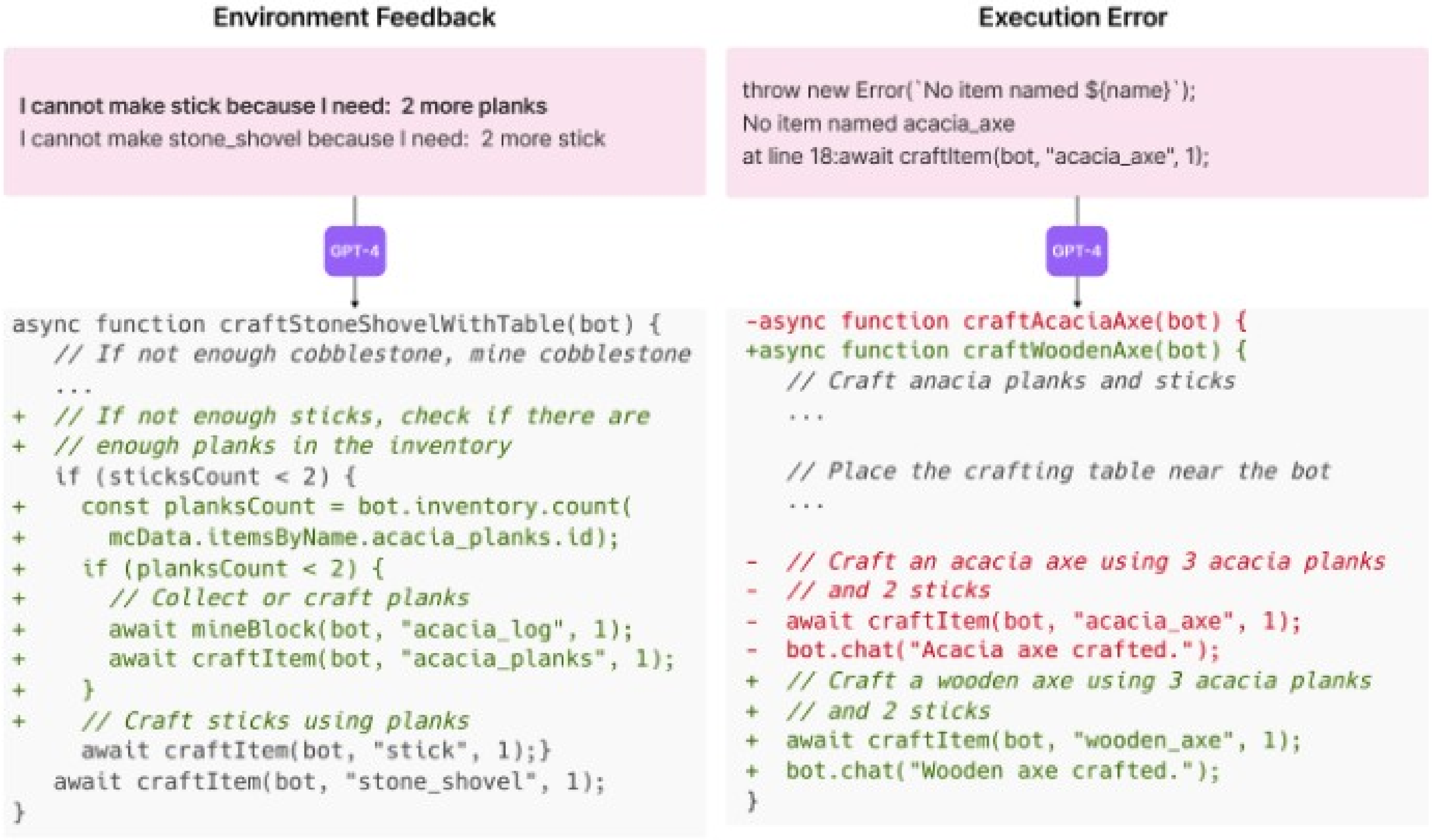
```
async function combatZombie(bot) {
  // Equip a weapon
  const sword =
bot.inventory.findInventoryItem(
    mcData.itemsByName[
      "stone_sword"
    ].id
  );
  if (sword) {
    await bot.equip(sword, "hand");
  } else {
    await craftStoneSword(bot);
    ...
  }
  // Craft and equip a shield
  ...
  // Recover hunger
  ...
  // Look for and combat a zombie
  ...
}
```

```
async function combatZombie(bot) {
  // The function is about
equipping a stone sword to combat
a zombie. If a stone sword is not
found, it will craft one.
Additionally, it crafts and equips
a shield for added protection.
Afterwards, it proceeds to cook
sticks in order to restore hunger.
Once hunger is replenished, it
actively searches for a zombie and
engages in combat with it.
}
```

How to craft an iron pickaxe in Minecraft?

To craft an iron pickaxe, you need to 3 iron ingots and 2 sticks. Once you have gathered the materials, ...

Skill library. Top: Adding a new skill. Each skill is indexed by the embedding of its description, which can be retrieved in similar situations in the future. **Bottom: Skill retrieval.** When faced with a new task proposed by the automatic curriculum, we perform querying to identify the top-5 relevant skills. Complex skills can be synthesized by composing simpler programs, which compounds Voyager's capabilities rapidly over time and alleviates catastrophic forgetting.



I cannot make stick because I need: 2 more planks
I cannot make stone_shovel because I need: 2 more stick

```
async function craftStoneShovelWithTable(bot) {
   // If not enough cobblestone, mine cobblestone
   ...
+  // If not enough sticks, check if there are
+  // enough planks in the inventory
   if (sticksCount < 2) {
+    const planksCount = bot.inventory.count(
+      mcData.itemsByName.acacia_planks.id);
+    if (planksCount < 2) {
+      // Collect or craft planks
+      await mineBlock(bot, "acacia_log", 1);
+      await craftItem(bot, "acacia_planks", 1);
+    }
+    // Craft sticks using planks
     await craftItem(bot, "stick", 1);}
   await craftItem(bot, "stone_shovel", 1);
}
```

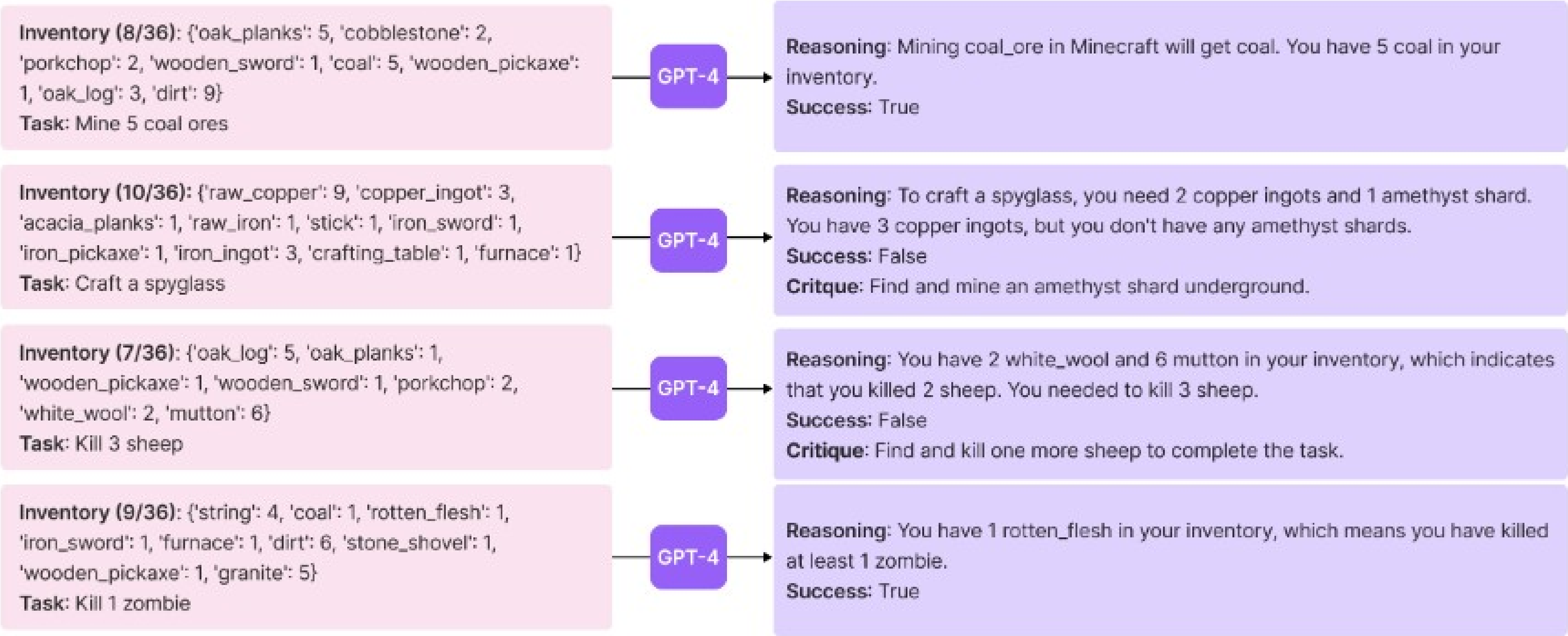
```
throw new Error(`No item named ${name}`);
No item named acacia_axe
at line 18:await craftItem(bot, "acacia_axe", 1);
```

```
-async function craftAcaciaAxe(bot) {
+async function craftWoodenAxe(bot) {
   // Craft anacia planks and sticks
   ...

   // Place the crafting table near the bot
   ...

-  // Craft an acacia axe using 3 acacia planks
-  // and 2 sticks
-  await craftItem(bot, "acacia_axe", 1);
-  bot.chat("Acacia axe crafted.");
+  // Craft a wooden axe using 3 acacia planks
+  // and 2 sticks
+  await craftItem(bot, "wooden_axe", 1);
+  bot.chat("Wooden axe crafted.");
}
```

Left: Environment feedback. GPT-4 realizes it needs 2 more planks before crafting sticks. **Right: Execution error.** GPT-4 realizes it should craft a wooden axe instead of an acacia axe since there is no acacia axe in Minecraft.



Inventory (8/36): {'oak_planks': 5, 'cobblestone': 2, 'porkchop': 2, 'wooden_sword': 1, 'coal': 5, 'wooden_pickaxe': 1, 'oak_log': 3, 'dirt': 9}
Task: Mine 5 coal ores

Reasoning: Mining coal_ore in Minecraft will get coal. You have 5 coal in your inventory.
Success: True

Inventory (10/36): {'raw_copper': 9, 'copper_ingot': 3, 'acacia_planks': 1, 'raw_iron': 1, 'stick': 1, 'iron_sword': 1, 'iron_pickaxe': 1, 'iron_ingot': 3, 'crafting_table': 1, 'furnace': 1}
Task: Craft a spyglass

Reasoning: To craft a spyglass, you need 2 copper ingots and 1 amethyst shard. You have 3 copper ingots, but you don't have any amethyst shards.
Success: False
Critque: Find and mine an amethyst shard underground.

Inventory (7/36): {'oak_log': 5, 'oak_planks': 1, 'wooden_pickaxe': 1, 'wooden_sword': 1, 'porkchop': 2, 'white_wool': 2, 'mutton': 6}
Task: Kill 3 sheep

Reasoning: You have 2 white_wool and 6 mutton in your inventory, which indicates that you killed 2 sheep. You needed to kill 3 sheep.
Success: False
Critique: Find and kill one more sheep to complete the task.

Inventory (9/36): {'string': 4, 'coal': 1, 'rotten_flesh': 1, 'iron_sword': 1, 'furnace': 1, 'dirt': 6, 'stone_shovel': 1, 'wooden_pickaxe': 1, 'granite': 5}
Task: Kill 1 zombie

Reasoning: You have 1 rotten_flesh in your inventory, which means you have killed at least 1 zombie.
Success: True

Self-verification. By providing the agent's current state and the task to GPT-4, we ask it to act as a critic and inform us whether the program achieves the task. In addition, if the task fails, it provides a critique by suggesting how to complete the task.