



TaskWeaver: A Code-First Agent Framework

Bo Qiao* **Liqun Li*** **Xu Zhang*** **Shilin He*** **Yu Kang** **Chaoyun Zhang**
Fangkai Yang **Hang Dong** **Jue Zhang** **Lu Wang** **Minghua Ma** **Pu Zhao** **Si Qin**
Xiaoting Qin **Chao Du** **Yong Xu** **Qingwei Lin** **Saravan Rajmohan**

Dongmei Zhang
Microsoft
taskweaver@microsoft.com

Abstract

Large Language Models (LLMs) have shown impressive abilities in natural language understanding and generation, leading to their use in applications such as chatbots and virtual assistants. However, existing LLM frameworks face limitations in handling domain-specific data analytics tasks with rich data structures. Moreover, they struggle with flexibility to meet diverse user requirements. To address these issues, TaskWeaver is proposed as a code-first framework for building LLM-powered autonomous agents. It converts user requests into executable code and treats user-defined plugins as callable functions. TaskWeaver provides support for rich data structures, flexible plugin usage, and dynamic plugin selection, and leverages LLM coding capabilities for complex logic. It also incorporates domain-specific knowledge through examples and ensures the secure execution of generated code. TaskWeaver offers a powerful and flexible framework for creating intelligent conversational agents that can handle complex tasks and adapt to domain-specific scenarios. The code is open-sourced at <https://github.com/microsoft/TaskWeaver/>.

1 Introduction

Large Language Models (LLMs), such as GPT [18, 12], Claude [11], Palm [10], and Llama [19], have demonstrated remarkable capabilities in natural language understanding and generation. These models have been widely used in various applications, including chatbots, virtual assistants, and content-generation systems. There is a growing potential for LLMs to revolutionize the way humans interact with machines, providing a more natural and intuitive experience.

An agent, specifically those that utilize Large Language Models (LLMs) or other AI technologies, is regarded as an autonomous entity that possesses the ability to plan tasks, observe its surroundings, and execute appropriate actions accordingly [20, 22]. Several existing frameworks, including Langchain [6], Semantic Kernel [8], Transformers Agent [9], Agents [25], AutoGen [1], and JARVIS [5], have endeavored to utilize LLMs for task-oriented conversations. These frameworks enable users to interact with LLM-powered agents by issuing natural language requests and receiving responses in return. Nevertheless, these frameworks possess limitations that constrain their efficacy in handling domain-specific scenarios and data analytics tasks.

*Equal Contribution

One major limitation is that most existing frameworks lack native support to handle rich data structures. LLM-powered agents often need to work with complex data structures, such as nested lists, dictionaries, or data frames, for data analytics applications and many other business scenarios. However, many of existing frameworks struggle to handle these structures efficiently, particularly when it comes to transferring information between chat rounds or across different plugins. In such cases, these frameworks either persist data to disk or encode complex structures as strings or JSON objects in the prompts. Although these approaches are functional, they can lead to impracticality and increased error rates, particularly when dealing with large datasets.

Another limitation of existing approaches is the lack of configuration for incorporating domain knowledge. While these frameworks provide tools and examples for prompt engineering, they fail to offer a systematic way to embed domain-specific knowledge into the planning and code-generation process. Consequently, the limitation makes it challenging to control the planning and code generation process in accordance with specific domain requirements.

Another issue encountered in many existing frameworks is their inflexibility, which hinders the ability to meet the diverse requirements of users. Although plugins can address common needs, they may fall short when it comes to handling ad-hoc queries. Writing a separate plugin for each ad-hoc query is impractical. In these situations, it becomes necessary for the agent to be able to write custom code to execute the user’s query. Therefore, there is a need for a solution that seamlessly integrates plugin execution with custom code execution to address this issue.

To address these limitations, we propose TaskWeaver, a code-first framework for building LLM-powered autonomous agents. The standout feature of TaskWeaver is its ability to convert each user request into executable code, treating user-defined plugins as callable functions. TaskWeaver overcomes the limitations of existing frameworks by providing support for rich data structures, flexible plugin usage, and dynamic plugin selection. It leverages the coding capability of LLMs to implement complex logic and incorporates domain-specific knowledge through examples. Additionally, TaskWeaver has made considerable efforts towards the secure execution of generated code and provides an easy-to-use interface for developers.

In this paper, we present the design and implementation of TaskWeaver, along with several case studies that demonstrate its effectiveness in handling various tasks. Overall, TaskWeaver provides a powerful and flexible framework for building intelligent conversational agents that can handle complex tasks and adapt to domain-specific scenarios.

2 Motivation and Requirements

To illustrate the TaskWeaver approach, let’s consider a real-world use case – conducting anomaly detection on time series data stored in an SQL database. Our goal is to apply a specialized anomaly detection algorithm to this data, requiring two input columns of types timestamp and float, respectively. The expected conversation between the user and the AI assistant proceeds as follows:

The example demonstrates common actions in a data analysis task, which include obtaining data, performing analysis on the data, and visualizing the results. By examining the steps in this use case, we can identify key requirements imposed by this example:

- **Plugin:** TaskWeaver must support invoking custom plugins. In this example, plugins are needed to pull data from the database and implement the specialized anomaly detection algorithm.
- **Rich data structure:** TaskWeaver must be capable of handling data in complex structures, such as pandas DataFrame, to perform advanced data processing actions. Data in rich structure should be able to transfer easily from one plugin to another.
- **Stateful execution:** TaskWeaver engages in iterative interactions with the user, processing user inputs and executing tasks accordingly. The execution state is preserved throughout the entire conversation session across multiple chat rounds.
- **Reasoning and action (React):** TaskWeaver is unaware of the data schema stored in the database prior to reading it. To generate the anomaly detection code, TaskWeaver must first inspect the data schema and then input the corresponding column names into the anomaly detection algorithm.

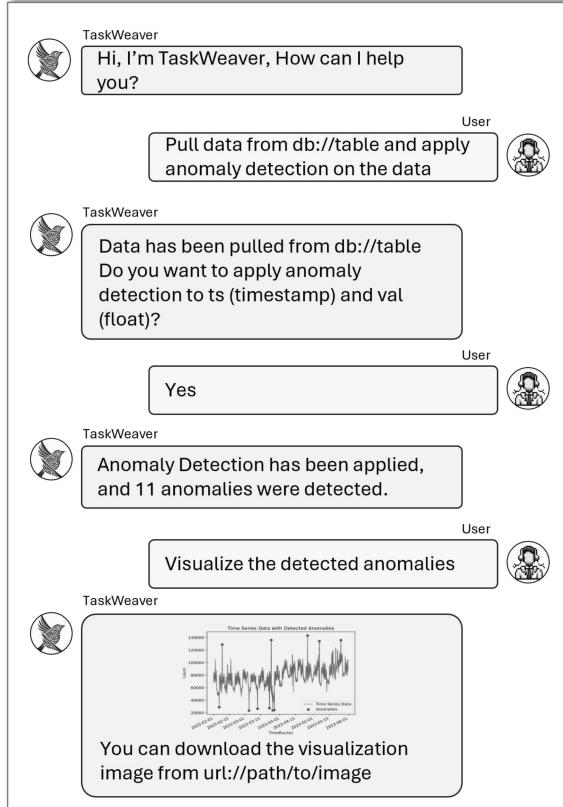


Figure 1: Chat between the user and the assistant.

- Response in natural language: TaskWeaver consistently responds to the user in human-readable natural language. Generally, the anomaly detection algorithm returns a DataFrame, but TaskWeaver needs to provide a summary of the execution result, such as “*11 anomalies were detected*”.
- Code generation: TaskWeaver must generate code to accommodate ad-hoc user demands, which are not covered by the pre-defined plugins. In the example provided, TaskWeaver generates code to visualize the detected anomalies.
- Incorporating domain knowledge: TaskWeaver should provide a systematic way to incorporate domain-specific knowledge. It would help LLMs make better planning and accurate tool calls, which in turn produces reliable results, particularly in complex domains.
- Persisting artifact: TaskWeaver should offer a means of saving results, such as DataFrames or images, to persistent storage. Users can download the artifacts via the provided links.

We have so far summarized the requirements from our motivating example. In the following section, we are going to describe the design of TaskWeaver.

3 A Glance of TaskWeaver

Fig. 2 presents an overview of TaskWeaver, which consists of three key components: the *Planner*, *Code Generator* (CG), and *Code Executor* (CE). The Code Generator and Code Executor consist of the Code Interpreter (CI). The Planner serves as the system’s entry point and interacts with the user. Its responsibilities include: (1) planning – breaking down the user’s request into subtasks and managing the execution process with self-reflection; and (2) responding – transforming the execution result into a human-readable response for the user. The CG generates code for a given subtask from the Planner, considering existing plugins to enable the generated code to incorporate function calls for specific tasks. The examples within the CG guide it, particularly for domain-specific tasks unfamiliar

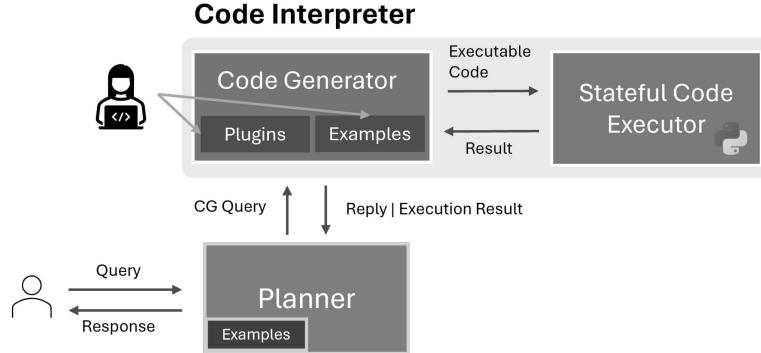


Figure 2: The overview of TaskWeaver

to the LLM. Lastly, the CE is responsible for executing the generated code and maintaining the execution state throughout the entire session.

Recall that we have motivated our design with an example of pulling data from a database and applying a custom anomaly detection algorithm to the data. We now explain how a sub-task of it is accomplished in TaskWeaver. The workflow is illustrated in Fig. 3. The prompts shown in Fig. 3 is simplified and only for illustration purpose due to the space limitation. The actual ones are much more complicated.

The initial step involves the Planner taking the user query, Code Interpreter (CI) description, and, if provided, planning examples to generate a plan. The CI description outlines its code generation and execution capabilities. To enhance the Planner’s effectiveness in task planning, the description includes details of the available plugins. The output of the Planner is a step-by-step plan, according to which the Planner phrases the queries and communicates with the CI. The first step (highlighted) consists of pulling data from the database and describing the data schema.

The Code Generator (CG) prompt delineates its profile and competencies, providing comprehensive definitions of all the relevant plugins. This includes the function name, its description, the arguments it accepts, and what it returns. Additionally, code generation examples may be incorporated into the prompt to steer the code generation process. The output from the CG is a code snippet that executes the `sql_pull_data` plugin, retrieves the data into a DataFrame, and provides a description of the data schema.

The Code Executor (CE)’s execution result is sent back to the Planner to determine the next step in the plan. In practice, the Planner may modify its original plan if the outcome differs from expectations. In our example, the execution result reveals two columns, namely `date` and `value`, in the DataFrame. For the next step, the Planner can either confirm with the user if these columns correspond to the two input parameters `ts_col` and `val_col` of the `anomaly_detection` plugin, or directly proceed to the third step, as it is reasonable to assume that `date` and `value` likely represent `ts_col` and `val_col`, respectively. Regardless, TaskWeaver must first retrieve the data and understand its schema before making a decision for the second step, which involves a self-reflection process.

As shown in this example, TaskWeaver incorporates a two-layer planning process during the handling of user requests. The first layer consists of the Planner generating a high-level plan outlining the steps required to fulfill the request. Subsequently, in each round, the code generator must devise a plan, in terms of chain-of-thought and generated code, to execute the specified step.

3.1 Terminology

We introduce the terminology in this paper.

Session A new *session* is established once the user submits their initial request to the TaskWeaver. This session is terminated if the user intentionally resets the conversation or when a predetermined expiration time is reached following the last interaction.

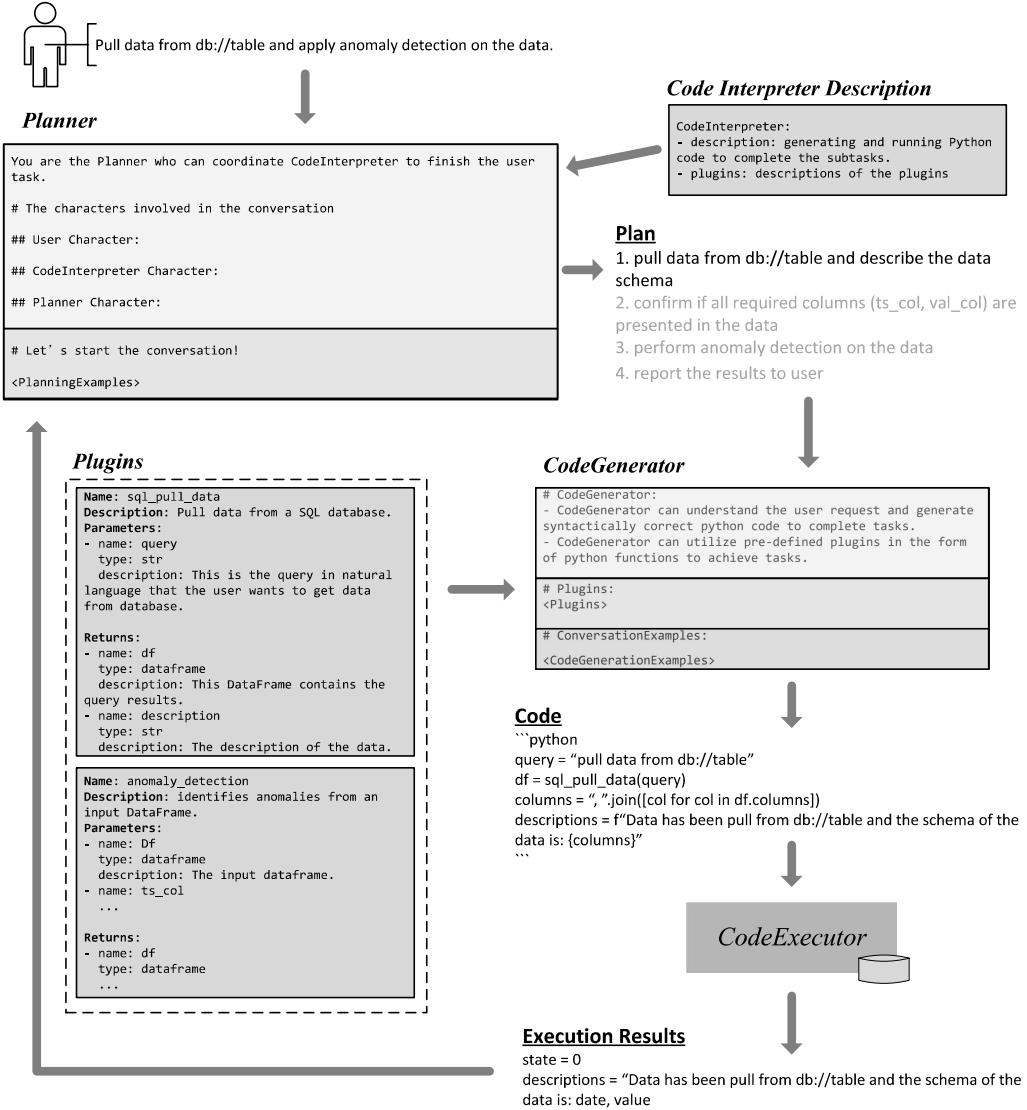


Figure 3: Workflow of TaskWeaver

Round A *round* commences with TaskWeaver receiving a user request and concludes upon providing a response to the user. Subsequently, TaskWeaver awaits the user’s next input. Typically, a session consists of numerous rounds. Responses to the user may either involve a message after completing a specific task or TaskWeaver requesting further input to successfully carry out the task.

Post Within a round, there can be several messages exchanged between the Planner, CG, and CE, each of which is referred to as a *post*. A post contains the text message, such as the request from the Planner to CG for code generation, and may also include other relevant information like the generated code and execution logs.

State TaskWeaver retains essential information throughout the conversation, known as the *state* (or context) of the session. The state encompasses the chat history between the user and TaskWeaver, the model’s internal thoughts and plans, generated code, execution results, and more. The session state functions as a short-term memory for the LLM, guiding it towards making appropriate decisions.

4 Design Considerations

In this section, we discuss the design considerations.

4.1 Code-First Analysis Experience

Python has emerged as the de-facto language for data analysis, and TaskWeaver leverages this popularity by converting user requests into Python programs that run on dedicated processes. Users can issue natural language requests to manipulate the state of the Python process with TaskWeaver, which utilizes popular libraries like numpy, pandas, sklearn, etc. Unlike other frameworks that rely on text or file-based expressions, TaskWeaver utilizes native data structures such as pandas DataFrame. This makes it easy to perform tasks such as pulling data from a database, running machine learning algorithms (e.g., anomaly detection, classification or clustering), summarizing results, and visualizing analysis outcomes.

4.2 Restricted Code Generation

The TaskWeaver approach involves a process of code verification (before code execution) to ensure that the generated code conforms to pre-defined rules and does not violate any safety requirements. This is achieved through the use of configurable rules that can be customized to suit different scenarios. By doing so, users can ensure that the code does not import any forbidden packages or invoke any unsafe functions. This verification process not only addresses safety concerns, but also supports plugin-only mode functionality where only the plugin functions can be called, and all other generated code is denied.

4.3 Stateful Code Execution

When users make ad-hoc requests for data analysis, it often involves multiple iterations. As a result, TaskWeaver needs to maintain the state of code execution throughout the entire session. This is similar to programming in Python using Jupyter Notebook, where users type code snippets in a sequence of cells and the program’s internal state progresses sequentially. However, in TaskWeaver, users use natural language instead of a programming language. TaskWeaver converts each user request into one or more code snippets in each round, depending on the specific plan.

4.4 Intelligent Plan Decomposition

The Planner decomposes users’ requests into sub-tasks that are simplified and executable by the Code Interpreter. We identified three types of dependencies between different sub-tasks: sequential, interactive, and none. Sub-task B is sequentially dependent on sub-task A means that B must run after A is done. Interactive dependency is the same as sequential in the execution order. More than that, it means there is a need for intervention by a human or a LLM between the two sub-tasks. For example, the user instructs TaskWeaver to read a file and follow the instructions in its content. The Planner split the request into 2 steps: (1) read the file content; (2) follow the instructions. The LLM needs to complete the first step to read the content before carrying out the second step. The third type of dependency is none which means there is no dependency there and they can be conducted in parallel. According to this definition, two steps where one sequentially depends on the other could be merged into one step for code generation because no intervention is required. In TaskWeaver, the Planner involves two-phase planning, where we enforce it to reconsider the generated plan of sub-tasks to merge sub-tasks with sequential dependency. This can prevent the model from splitting the request into too fine-grained steps leading to a prolonged execution process and incurring unnecessary costs (call the LLM many times).

4.5 Self-Reflection

TaskWeaver is designed with the capacity to rectify errors throughout the planning and code generation stages. When it detects that the outcomes of the preceding steps diverge from the anticipated results, the Planner possesses the capability to reassess and modify its plan, exploring alternative approaches. Furthermore, the Code Interpreter (CI) is equipped to evaluate the results of code execution. Should the code execution process encounter an exception or the code fails to pass the verification, the CI

can initiate a re-generation of the code, thereby attempting to correct the code. This iterative process ensures that TaskWeaver maintains a robust and adaptable approach to task execution, increasing the reliability and efficiency of the framework.

4.6 Scalable Plugin Usage

In TaskWeaver, plugins are specialized Python functions used to handle tasks that are either too complex or require specific domain knowledge, thereby eliminating the number of plugins needed since TaskWeaver can already handle general Python code generation. Furthermore, TaskWeaver features dynamic plugin selection. This means that after a user request is received, only the plugins that are relevant to that request are selected from a pool of available plugins. This approach ensures that TaskWeaver uses the most appropriate tools for the task at hand without overloading the prompt with unnecessary functions.

4.7 Incorporating Domain Knowledge

One way to incorporate domain knowledge is by defining custom plugins, as discussed previously. However, for domain-specific tasks, it can be challenging for the LLM to generate the correct code to call the plugins or to make a good plan. To address this, we have introduced an interface in TaskWeaver that allows users to guide the system for such difficult tasks. TaskWeaver enables users to configure examples to teach the LLM how to respond to certain requests. For instance, a conversation history containing step-by-step thoughts and request/response sections can be used as an example. There are two types of examples in TaskWeaver: one is used for planning and the other for code generation. By using examples, TaskWeaver can incorporate domain-specific knowledge and improve the LLM’s ability to generate accurate plans and code for difficult tasks.

4.8 Security

Executing freely generated code can introduce security risks. For example, a malicious user may ask TaskWeaver to open a file containing security keys, delete system files, or terminate a process. A typical way to mitigate the security risks is to include certain statements in the prompts to the LLM, which is implemented in TaskWeaver. To prevent these malicious behaviors, TaskWeaver allocates a separate worker process for each session, and each worker process is independent of other processes under a special OS user. As a result, the worker process is unable to access files or other processes beyond the OS user’s scope, thus preventing any malicious behavior. The worker processes are communicated via an inter-process interface. In the future, we plan to support running each worker process in a sandbox to further enhance the security of the system.

4.9 Easy to Use

Existing LLM frameworks such as Langchain make it easy to build proof-of-concept demos. However, building a reliable system with these frameworks can be time-consuming due to the large number of components they provide (like a large box of lego bricks). One of the main goals of TaskWeaver is to make it easy to use. Typically, users only need to customize the plugins to get started. For more difficult tasks, users can customize the examples for code generation and planning. To aid users, TaskWeaver includes various tools to help, such as a tool to convert Python functions into plugins and a tool to save existing conversations as examples. These tools make it easier for users to customize the system. Another key feature of TaskWeaver is its support for multi-tenant open box. The system implements a session manager to isolate different user sessions, making it easy to serve multiple users at once. This enables the system to be used as a service, supporting a wide range of use cases.

4.10 LLM Cost

The cost of calling LLMs can be significant, and TaskWeaver addresses this issue by letting different modules be configured with different LLM models. For instance, GPT 3.5 is much cheaper compared to GPT 4. Therefore, for simpler tasks, we may use a cheaper model to reduce the overall cost. Second, we have carefully analyzed the process in TaskWeaver and incorporated a set of rules to bypass calling the LLM under certain conditions.

5 TaskWeaver in Detail

We are going to explain each module in one section accordingly.

5.1 Planner

The Planner serves as a crucial component in the TaskWeaver system, where it decomposes requests from users into several sub-tasks and orchestrates capabilities within TaskWeaver to complete the task and report back to the users. From a high-level perspective, the Planner functions as the entry point and controller, managing the entire system. As illustrated in Figure 2, the Planner communicates bidirectionally with each component, sending queries and receiving responses.

As shown in Fig. 3, a typical working routine of the Planner is as follows: The Planner first receives a query from users and then decides to decompose it into multiple sub-tasks. These sub-tasks essentially form a “Initial Plan”, which is generated based on the knowledge of LLMs or enhanced by domain-specific “Examples”. After drafting the initial plan, the Planner is requested to refine this initial plan by considering the dependencies among the sub-tasks as discussed in Sec. 4.4 in a chain-of-thought manner. The Planner may merge sub-tasks into one in its “Final Plan”. Table 1 shows two examples of the Planner’s initial plan and final plan w.r.t the User’s request. In the first example, the initial plan has 4 steps while the first 3 steps are merged into one in the final plan. In the second example, the final plan is the same as the initial plan because the Planner needs to read the file content and then understand what would be the next step.

User request: Load data from a.csv, show the column names, and count the number of rows	
Initial Plan	Final Plan
<ol style="list-style-type: none">1. load a.csv2. extract and display the column names <sequentially depends on 1>3. count the number of rows <sequentially depends on 1>4. report the information to the user <interactively depends on 2,3>	<ol style="list-style-type: none">1. load a.csv, extract the column names, and count the number of rows2. report the information to the user

User request: Read file manual.txt and follow the instructions in it	
Initial Plan	Final Plan
<ol style="list-style-type: none">1. read manual.txt and show its content2. follow the instructions according to the file content <interactively depends on 1>3. report the result to the user <interactively depends on 2>	<ol style="list-style-type: none">1. read manual.txt and show its content2. follow the instructions according to the file content3. report the result to the user

Table 1: Two examples of the initial plans and the corresponding final plans.

After the plan is finalized, the Planner takes action by assigning each sub-task, with phrased queries, to ask the CI to generate a code snippet, leveraging in-domain plugins when necessary. The execution results are sent back to the Planner. Following the ReAct (reasoning and act) design pattern, upon observing the execution results, the Planner may update its plan, request additional information from users, and so on. The process is repeated for subsequent sub-tasks until the entire plan is completed.

When addressing domain-specific scenarios where the LLM’s own knowledge is insufficient, the Planner can incorporate external knowledge with “Examples”. These examples are tailored by scenario developers according to their usage requirements. One example is essentially the chat history between the User, the Planner, and the Code Interpreter, including the plans of the Planner. The Examples could be saved from an online conversation for the purpose of stabilizing the planning

process for future requests, or they could be manually prepared. A real planning Example is provided in Appendix B.

5.2 Code Generator (CG)

Code Generator is designed to utilize LLMs to automatically synthesize a Python code snippet based on an incoming request. From a high-level view, CG combines the benefits of both the plugin system and code interpreter, allowing the capability of invoking plugins and generating additional code. Inside the CG, plugins and examples customized by users are leveraged to generate the code.

1. **Plugin:** In general, plugins can take on various forms such as a web API call, a software module, a customized algorithm, or a deep learning model. Regardless of the form, all variants can be invoked by a function call. Therefore, we have encapsulated the plugins as a Python function within the Code Generator for seamless invocation.
2. **Example:** To aid the LLMs in adapting to domain-specific scenarios, examples are designed to help guide LLMs to behave by following the examples. Examples act as a guide for the LLMs to follow and improve their performance by providing contextualized examples. This feature ensures that the generated code aligns with the specific requirements of the user's domain. A real code generation Example is provided in Appendix C.

The CG has the ability to generate code that exclusively calls upon plugins, code that does not use any plugins, or a combination of both. The code that doesn't depend on plugins is specifically tailored to handle requests that cannot be met using only existing plugins. In the motivating example presented in Section 2, there is a plugin called 'anomaly_detection' that can identify anomalies in data. In this scenario, the CG would first invoke the plugin through a single line of code. Subsequently, the CG would generate multiple lines of additional code to visualize the detected anomalies, as requested by the user.

The knowledge of LLMs is often limited, particularly in domain-specific scenarios. In many cases, there are in-domain tools better suited for completing a specific task. Therefore, the Plugin system can enhance LLMs by enabling them to leverage existing tools. The Plugin system consists of the following two components:

1. **Plugin Schema** LLMs need to understand the capabilities of a plugin, including its arguments and return values. This information is embedded in the plugin schema file (in YAML format) and could be customized by users. The plugin schema comprises the name, metadata, plugin description, arguments, and return values. For each argument and return value, users should provide its name, type, and description. The plugin schema is then supplied to LLMs as part of the prompt to generate the code.
2. **Plugin Implementation** The plugin implementation defines how each plugin is executed using Python in Code Executor, where the arguments and return values should correspond with the Plugin Schema. Various plugins can be implemented in Python code, such as a domain-specific algorithm, a software module, a deep learning model or a Web API call. It is important to note that LLMs do not need to know the plugin implementation details to generate code. On the contrary, the Plugin Schema is used for code generation.

Appendix D shows an example of the plugin schema and implementation.

5.2.1 Examples

Adapting Large Language Models (LLMs) to domain-specific scenarios presents a significant challenge in enabling LLMs to comprehend user queries and generate code for invoking plugins accurately and reliably. Without proper guidance, LLMs cannot acquire domain-specific knowledge, and therefore, they may fail to chain the appropriate plugins to complete a task. The Example system is designed to provide a conversation-level demonstration for LLMs to emulate its behavior. It follows a Chain-Of-Thoughts format before generating the code, which can be customized by users through a YAML file. The examples are also included as part of the prompt sent to LLMs in the Code Generator, alongside the plugin schema.

5.2.2 Post Verification

Even with explicit instructions added to the prompt, such as restricting the call to plugin functions, prohibiting local file system modifications, or disallowing certain package installations, the LLM may still generate code that disregards these instructions. This necessitates a post-verification process to ensure the generated code is safe to execute. Following code generation, the Code Generator (CG) parses the code into an Abstract Syntax Tree (AST) and examines it line by line for any violations. If violations are detected, an error message is reported, and a new code snippet is generated. The CG will retry this process a maximum of three times; if violations persist, the CG will notify the planner of its failure to generate compliant code.

5.2.3 Code Auto Correction

Code auto-correction shares similarities with the post-verification process. If the generated code fails to execute, the exception message is reported to the Code Generator (CG), prompting it to retry generating the code. The primary difference is that post-verification operates within the CG, while code auto-correction relies on the Code Executor to run the code and report errors. Notably, if the execution fails, the planner can directly redirect the message to the CG instead of synthesizing the report via the LLM. TaskWeaver permits the code to regenerate up to a maximum of three times.

5.3 Code Executor

The Code Executor (CE) receives the code generated by the Code Generator (CG), collects dependent modules and plugin definitions, executes it, preserves context information such as logs, and returns an execution result to the Planner. In TaskWeaver, we implement CE based on Python Jupyter. To prevent interference between different sessions, CE maintains a separate Jupyter process for each session. In future implementations, separate sandboxes (e.g., Docker containers) will be employed for improved isolation across sessions. When a session concludes, the Jupyter process is terminated. The execution result contains the following parts which are returned to the planner.

- **Return Code:** a successful code execution will return code 0 and otherwise 1.
- **Logs:** Logs are generated in two ways: (1) the stdout/stderr output of the program, and (2) log messages recorded using a logging utility within the plugins.
- **Output:** This is the output of the Jupyter cell running the generated code.
- **Artifacts:** The generated code or the plugin calls may produce artifacts such as a CSV file or an image. The user can download the artifacts via the provided URLs.

As discussed in Sec. 5.2.3, if the CE fails to execute the code from the CG, it will report the error logs to the CG, who would attempt to revise the code to fix the issue. All the error information and the failed code are kept in the CG's conversation history so that the CG is aware of the full execution history and can precisely understand the state of the CE.

6 Extension to Multi-Agents

This section briefly discusses the process of expanding the TaskWeaver to a multi-agent architecture. Extending to a multi-agent architecture benefits from several aspects. Firstly, it is a good practice to modularize a complex project into multiple agents, with each agent responsible for a specific set of functions. This is especially useful if there are a large number of plugins. Secondly, this is a good way to add new functions, by plugging in a new agent, to an existing project without modifying existing code.

There are two ways of extending the TaskWeaver in a multi-agent environment, as illustrated in Fig. 4. The first approach involves one agent (powered by TaskWeaver) calling other agents via its plugins. Fig. 4 (a) depicts a simple example, although this can be extended to a more complex network where multiple agents form a mesh network. The second approach involves embedding TaskWeaver-powered agents into an existing multi-agent framework, such as AutoGen [1], as demonstrated in Fig. 4 (b).

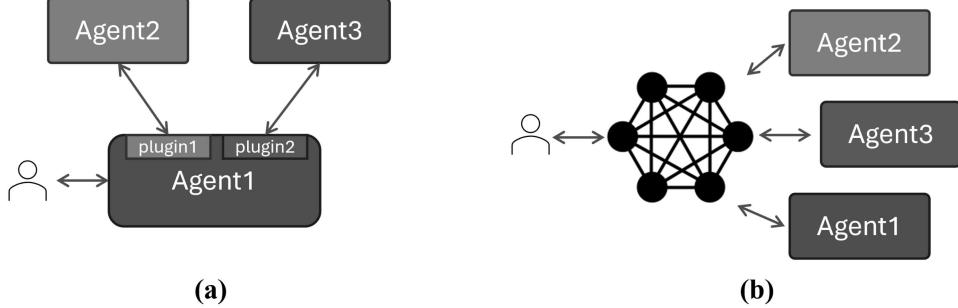


Figure 4: TaskWeaver in a multi-agent environment.

7 Case Studies

In this section, we demonstrate how to use TaskWeaver for practical tasks:

- Anomaly detection based on data pulled from a database
- Stock price forecasting

7.1 Task 1: Anomaly Detection

We aim to identify anomalies within a time series dataset stored in an SQL database (sqlite3). To accomplish this goal, we need to integrate the two plugins for data retrieval and time series anomaly detection:

- **pull_data_sql(nl_query) → sql, dataframe**: Given a natural language query, pull data from a database and return the result in a pandas DataFrame, along with the generated SQL query.
- **anomaly_detection → dataframe with anomalies, results description**: This plugin utilizes a straightforward 3-sigma algorithm to identify any abnormal data points in a time series. These data points deviate from the mean value by more than three standard deviations.

Note: There is no need to provide plugins for general tasks, such as reading or writing files, as the TaskWeaver is capable of generating the necessary code for these tasks. This is an advantage of TaskWeaver that reduces the development effort to bootstrap applications.

Fig.5 in Appendix A illustrated the detailed plan generated by the Planner of TaskWeaver:

1. Instruct CodeInterpreter to pull data from the time_series table in the database.
2. Confirm the columns to be detected anomalies.
3. Instruct CodeInterpreter to detect anomalies on the pulled data.
4. Report the detected anomalies to the user.

In the first step, the Code Interpreter invoked the *pull_data_sql* plugin function and automatically filled the required parameters.

```

1 from typing import Tuple
2 import pandas as pd
3
4 query = "SELECT * FROM time_series"
5 df, description = sql_pull_data(query)
6 df, description

```

After obtaining the time series data from the database, TaskWeaver asked the user to provide the column names as additional information to proceed with anomaly detection. The user then provided the "ts" and "val" column names to detect anomalies. With the additional information confirmed, TaskWeaver proceeded to execute the third step, i.e., detecting anomalies using the *anomaly_detection* plugin.

```

1 time_col_name = 'ts'
2 value_col_name = 'val'
3
4 anomaly_df, anomaly_description = anomaly_detection(df, time_col_name,
5           value_col_name)
anomaly_df, anomaly_description

```

In the end, 11 anomalies were detected and a response was composed for the user.

7.2 Task 2: Stock Price Forecasting

The user requested TaskWeaver to forecast the Nasdaq 100 (QQQ) index prices for the next seven days with the ARIMA model. The detailed execution process is shown in Fig.6 in Appendix A. Here is the plan generated by the TaskWeaver Planner:

1. Instruct CodeInterpreter to obtain historical QQQ stock price data.
2. Preprocess the data.
3. Train the ARIMA model.
4. Forecast the stock price for the next 7 days.
5. Report the predicted stock prices to the user.

After receiving the first subtask from the Planner, the Code Interpreter proceeded to generate a code snippet for the first step. The Code Interpreter thought to itself, "ProgramApe (internal code name) will generate a code snippet to load QQQ historical data using pandas_datareader library." The resulting code snippet is as follows:

```

1 import pandas_datareader as pdr
2 import datetime
3 start_date = datetime.datetime.now() - datetime.timedelta(days=365)
4 end_date = datetime.datetime.now()
5 qqq_data = pdr.get_data_yahoo('QQQ', start=start_date, end=end_date)
6 qqq_data

```

Nonetheless, the execution encountered a failure and the following error information was reported:

```

The execution of the generated python code above has failed
During execution, the following messages were logged:
-----
TypeError Traceback (most recent call last)
Cell In[1], line 7
4 start_date = datetime.datetime.now() - datetime.timedelta(days=365)
5 end_date = datetime.datetime.now()
----> 7 qqq_data = pdr.get_data_yahoo('QQQ', start=start_date, end=end_date
     )
8 qqq_data
File \path\to\python\Lib\site-packages\pandas_datareader\data.py:80, in
get_data_yahoo(*args, **kwargs)
79 def get_data_yahoo(*args, **kwargs):
---> 80     return YahooDailyReader(*args, **kwargs).read()
...

```

As a result, the Code Interpreter had to modify the code to resolve this issue.

```

1 # Import yfinance or install it if it's not available
2 try:
3     import yfinance as yf
4 except ImportError:
5     !pip install yfinance
6     import yfinance as yf

```

```

7
8 # Load the historical price data for QQQ
9 qqq_data = yf.download('QQQ')
10 qqq_data

```

In the aforementioned code, we can observe that TaskWeaver employed an alternative approach to search for stock price data using the yfinance library. This time, the historical QQQ stock price data was successfully downloaded and the results were forwarded to the Planner for further instructions.

The Planner received the downloaded stock price data and proceeded with the following steps of preprocessing and ARIMA model training. Ultimately, TaskWeaver utilized the fitted ARIMA model to predict the stock prices for the next 7 days.

8 Design Verification

In this section, we use a set of tasks to verify that the TaskWeaver meets our requirements and design considerations.

8.1 Planning

Task 1: React ReAct[23] merges Reasoning and Acting for LLMs, providing a comprehensive paradigm for generating verbal reasoning traces and actions to accomplish a given task. By leveraging this approach, the system can conduct real-time reasoning to create, update, and adapt plans while observing the external environments, to incorporate additional information into the reasoning process.

To evaluate the ReAct capabilities of TaskWeaver, we adopted an approach inspired by the Challenge Task presented in [3]. This involved generating a collection of N files with the naming convention file₁.txt, file₂.txt, ..., file_N.txt. Each file contained the instruction "read file_{i + 1}.txt in the same directory to get the further information." The goal was to initiate the TaskWeaver to begin reading file₁.txt and sequentially progress to the subsequent files. The final file in the sequence contained instructions to present a specific key to the user.

The results of the evaluation are illustrated as following:

```

Human: read the file_A.txt and follow the instructions in it
.....
>>> [PLANNER->CODEINTERPRETER]
Please read the content of the file file_A.txt
.....
>>> [CODEINTERPRETER->PLANNER]
The execution of the generated python code above has succeeded
The stdout is:
read file_B.txt in the same directory to get the further information.
.....
>>> [PLANNER->CODEINTERPRETER]
Please read the content of the file file_B.txt
.....
>>> [CODEINTERPRETER->PLANNER]
The execution of the generated python code above has succeeded
The stdout is:
read file_C.txt in the same directory to get the further information.
.....
>>> [PLANNER->CODEINTERPRETER]
Please read the content of the file file_C.txt

```

```

>>> [CODEINTERPRETER->PLANNER]
The execution of the generated python code above has succeeded
The result of above Python code after execution is: Show the key to user.
The key is 12345.
.....
>>> [PLANNER->USER]
The key is 12345.

```

In the depicted process, the Planner component of TaskWeaver initially broke down the task into two steps and initiated the execution of the first step. This initial phase involved reading the contents of the file_A.txt. Subsequently, the Code Interpreter received the Planner's request and generated a Python code snippet designed to extract the content from the specified file. The generated code included an instruction to "read file_B.txt in the same directory to acquire further information."

Upon receiving this instruction, the Planner updated the plan, incorporating the directive to load the next file in the sequence. This iterative process continued until TaskWeaver successfully navigated through the entire chain of files, culminating in the retrieval of the final message contained in the last file. This concluding message held instructions to present the key to the user, signifying the completion of the task.

Task 2: Plan Decomposition The Planner is capable of breaking down a task into multiple subtasks and delegating them to the Code Interpreter for execution one by one. However, given the cost and efficiency of LLM, it is not practical to invoke LLM multiple times, particularly for some simple tasks. For this reason, we devised a two-phase planning approach that mandates a review of the generated initial plan, for merging sub-tasks with sequential dependencies (refer to Sec.4.4 for more details).

As an illustration, we tasked TaskWeaver with computing the mean and standard deviation of the 'Count' column in the file "/sample_data/demo_data.csv" and subsequently verifying the presence of any values exceeding 3 standard deviations from the mean. The initial plan generated by the Planner is as follows:

- 1. Load the data file
- 2. Calculate the mean and std of the 'Count' column <sequentially depends on 1>
- 3. Check if there are any values larger than 3 std from the mean <sequentially depends on 2>
- 4. Report the result to the user <interactively depends on 3>

It is noteworthy that the first and second steps can be combined into a single step since they can be accomplished in a single snippet of code without any interventions. As a result, the Planner merged them into one: "Instruct CodeInterpreter to load the data file and calculate the mean and std of the 'Count' column." By doing so, we were able to reduce the number of LLM calls from 6 to 3 for the data loading and the mean/std value calculation.

8.2 Coding and Execution

Task 1: Plugin-Only Mode In the TaskWeaver, we offer a plugin-only mode, which exclusively permits the invocation of plugin functions and forbids the generation of arbitrary code. To validate this feature, we activate the plugin-only mode in the configuration file and instruct TaskWeaver to generate 10 random numbers. Since the "rand" and "random" functions are not implemented as plugin functions, the Code Interpreter refuses to generate the code due to the constraints. Even if the code were generated, the code verification module would still intercept the execution due to the prohibition of non-plugin functions.

```

Human: generate 10 random numbers
.....
>>> [THOUGHT]
Code Interpreter understands the user's request and the constraints.

```

```

However, generating random numbers requires the use of numpy or the random
module, which is not allowed in this case.
>>> [CODEINTERPRETER->PLANNER]
I'm sorry, but I cannot generate random numbers without using numpy or the
random
module, which are not allowed in this task. Please let me know if there's
anything
else I can help you with.
.....

```

Task 2: Stateful Execution The Code Interpreter is stateful, meaning it maintains execution states and variables within the same session. For example, we initially asked TaskWeaver to display the column names of `./sample_data/demo_data.csv`. Subsequently, we instructed TaskWeaver to execute an irrelevant task, such as “generate 10 random numbers.” Afterward, we requested the mean value of the “Count” column in the previously loaded data. The TaskWeaver identified the need to use data from the previous chat round and subsequently delivered an appropriate response.

Task 3: Auto Correction The Code Interpreter can make mistakes while generating Python code, resulting in execution failures for the executor. To address this, we prompt the Code Interpreter to revise its code based on the reported error information. We asked TaskWeaver to calculate the mean value of `sample_data/demo_data.csv`. The Code Interpreter initially generated incorrect code due to the absence of the data schema.

```

1 import pandas as pd
2
3 data_file_path = './../../sample_data/demo_data.csv'
4 df = pd.read_csv(data_file_path)
5 mean_value = df.mean()
6 mean_value

```

Upon revising the code, it automatically identifies the columns with numerical data types and calculates their average value successfully.

```

1 import pandas as pd
2
3 # Load the data file
4 data_file_path = './../../sample_data/demo_data.csv'
5 df = pd.read_csv(data_file_path)
6
7 # Calculate the mean value of the loaded data
8 mean_value = df.mean(numeric_only=True)
9 mean_value

```

8.3 Safety

Task 1: Preventing File Deletion and Secret Key Leakage To ensure the safety and security of the execution environment, we have developed a restricted list to prevent certain sensitive operations, which can be customized by developers. When requesting the TaskWeaver to delete a file in the system folder or retrieve the secret key from global environment variables, it declines to execute these tasks, as they are deemed high-risk operations.

9 Related Work

LLM and Prompt Engineering Recent advancements in natural language processing have been driven by large language models (LLMs) [24] such as GPT [12], GPT-4 [17], Palm [10], and Llama [19]. These models have not only revolutionized the field of natural language processing, but also how humans interact with machines through applications such as ChatGPT. LLMs are pre-trained on a vast amount of text data and then fine-tuned with reinforcement learning from human feedback

(RLHF) and Instruction Fine-Tuning (IFT) [12] to improve their response quality. To improve the performance of LLMs on reasoning and decision-making tasks, various prompting engineering methods have been proposed, including Chain-of-Thought (CoT) [21], zero-shot-CoT [14], and ReAct [23]. Some of these approaches have also been applied in TaskWeaver to enhance its performance.

Agent Recently, LLM-based agents have gained increasing attention. The fundamental concept is to utilize LLMs as the core controller to make human-like decisions by observing the environment, planning, and taking actions[7]. There are generally two types of agent systems: single-agent and multi-agent systems. The single-agent system focuses more on planning, observing, and acting within the single agent’s own capability, including AutoGPT[2] and LangChain Agents[6]. Conversely, the latter is more concentrated on leveraging multiple agents to work collaboratively. Typical examples include BabyAGI[4], MetaGPT[13], AutoGen[1], CAMEL[15], and Multi-agent Debate (MAD)[16]. Our TaskWeaver is a single-agent framework that focuses on converting user requests into code, even for plugin calls.

10 Conclusion

In this paper, we introduced TaskWeaver, a code-first framework for building LLM-powered autonomous agents that addresses the limitations of existing frameworks in handling rich data structures, incorporating domain knowledge, and offering flexibility. TaskWeaver’s standout feature is its ability to convert user requests into executable code while treating user-defined plugins as callable functions. This approach enables the seamless integration of plugin execution with custom code execution, catering to the diverse requirements of users and providing a more intuitive user experience. We presented the design and implementation of TaskWeaver, highlighting its support for complex data structures, flexible plugin usage, and intelligence task planning. We also demonstrated TaskWeaver’s ability to leverage the coding capability of LLMs to implement complex logic and incorporate domain-specific knowledge through examples. Furthermore, we discussed the efforts made towards the secure execution of generated code and the provision of an easy-to-use interface for developers. Through various case studies, we showcased the effectiveness of TaskWeaver in handling different tasks. Overall, TaskWeaver offers a powerful and flexible solution for building intelligent conversational agents. As LLMs continue to evolve and improve, TaskWeaver can facilitate more advanced and sophisticated applications.

References

- [1] Autogen. Available at: <https://github.com/microsoft/autogen>. Accessed on [11/22/2023].
- [2] Autogpt. Available at: <https://github.com/Significant-Gravitas/AutoGPT>. Accessed on [11/22/2023].
- [3] Autogpt challenge. Available at: https://github.com/Significant-Gravitas/AutoGPT/blob/master/docs/content/challenges/memory/challenge_a.md. Accessed on [11/22/2023].
- [4] Babyagi. Available at: <https://github.com/yoheinakajima/babyagi>. Accessed on [11/22/2023].
- [5] Jarvis. Available at: <https://github.com/microsoft/JARVIS>. Accessed on [11/22/2023].
- [6] Langchain. Available at: <https://www.langchain.com/>. Accessed on [11/22/2023].
- [7] Llm powered autonomous agents. Available at: <https://lilianweng.github.io/posts/2023-06-23-agent/>. Accessed on [11/22/2023].
- [8] Semantic kernel. Available at: <https://github.com/microsoft/semantic-kernel>. Accessed on [11/22/2023].
- [9] Transformers agents. Available at: https://huggingface.co/docs/transformers/transformers_agents. Accessed on [11/22/2023].

- [10] Rohan Anil, Andrew M Dai, Orhan Firat, Melvin Johnson, Dmitry Lepikhin, Alexandre Passos, Siamak Shakeri, Emanuel Taropa, Paige Bailey, Zhifeng Chen, et al. Palm 2 technical report. *arXiv preprint arXiv:2305.10403*, 2023.
- [11] Amanda Askell, Yuntao Bai, Anna Chen, Dawn Drain, Deep Ganguli, Tom Henighan, Andy Jones, Nicholas Joseph, Benjamin Mann, Nova DasSarma, Nelson Elhage, Zac Hatfield-Dodds, Danny Hernandez, Jackson Kernion, Kamal Ndousse, Catherine Olsson, Dario Amodei, Tom B. Brown, Jack Clark, Sam McCandlish, Chris Olah, and Jared Kaplan. A general language assistant as a laboratory for alignment. *CoRR*, abs/2112.00861, 2021.
- [12] Tom Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared D Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, et al. Language models are few-shot learners. *Advances in neural information processing systems*, 33:1877–1901, 2020.
- [13] Sirui Hong, Xiawu Zheng, Jonathan Chen, Yuheng Cheng, Ceyao Zhang, Zili Wang, Steven Ka Shing Yau, Zijuan Lin, Liyang Zhou, Chenyu Ran, et al. Metagpt: Meta programming for multi-agent collaborative framework. *arXiv preprint arXiv:2308.00352*, 2023.
- [14] Takeshi Kojima, Shixiang Shane Gu, Machel Reid, Yutaka Matsuo, and Yusuke Iwasawa. Large language models are zero-shot reasoners. *Advances in neural information processing systems*, 35:22199–22213, 2022.
- [15] Guohao Li, Hasan Abed Al Kader Hammoud, Hani Itani, Dmitrii Khizbulin, and Bernard Ghanem. Camel: Communicative agents for "mind" exploration of large scale language model society. *arXiv preprint arXiv:2303.17760*, 2023.
- [16] Tian Liang, Zhiwei He, Wenxiang Jiao, Xing Wang, Yan Wang, Rui Wang, Yujiu Yang, Zhaopeng Tu, and Shuming Shi. Encouraging divergent thinking in large language models through multi-agent debate. *arXiv preprint arXiv:2305.19118*, 2023.
- [17] OpenAI. Gpt-4 technical report. *ArXiv*, abs/2303.08774, 2023.
- [18] Alec Radford, Karthik Narasimhan, Tim Salimans, and Ilya Sutskever. Improving language understanding with unsupervised learning. *OpenAI Blog*, 2018.
- [19] Hugo Touvron, Thibaut Lavril, Gautier Izacard, Xavier Martinet, Marie-Anne Lachaux, Timothée Lacroix, Baptiste Rozière, Naman Goyal, Eric Hambro, Faisal Azhar, et al. Llama: Open and efficient foundation language models. *arXiv preprint arXiv:2302.13971*, 2023.
- [20] Lei Wang, Chen Ma, Xueyang Feng, Zeyu Zhang, Hao Yang, Jingsen Zhang, Zhiyuan Chen, Jiakai Tang, Xu Chen, Yankai Lin, et al. A survey on large language model based autonomous agents. *arXiv preprint arXiv:2308.11432*, 2023.
- [21] Jason Wei, Xuezhi Wang, Dale Schuurmans, Maarten Bosma, Fei Xia, Ed Chi, Quoc V Le, Denny Zhou, et al. Chain-of-thought prompting elicits reasoning in large language models. *Advances in Neural Information Processing Systems*, 35:24824–24837, 2022.
- [22] Zhiheng Xi, Wenxiang Chen, Xin Guo, Wei He, Yiwen Ding, Boyang Hong, Ming Zhang, Junzhe Wang, Senjie Jin, Enyu Zhou, et al. The rise and potential of large language model based agents: A survey. *arXiv preprint arXiv:2309.07864*, 2023.
- [23] Shunyu Yao, Jeffrey Zhao, Dian Yu, Nan Du, Izhak Shafran, Karthik Narasimhan, and Yuan Cao. React: Synergizing reasoning and acting in language models. *arXiv preprint arXiv:2210.03629*, 2022.
- [24] Wayne Xin Zhao, Kun Zhou, Junyi Li, Tianyi Tang, Xiaolei Wang, Yupeng Hou, Yingqian Min, Beichen Zhang, Junjie Zhang, Zican Dong, et al. A survey of large language models. *arXiv preprint arXiv:2303.18223*, 2023.
- [25] Wangchunshu Zhou, Yuchen Eleanor Jiang, Long Li, Jialong Wu, Tiannan Wang, Shi Qiu, Jintian Zhang, Jing Chen, Ruipu Wu, Shuai Wang, et al. Agents: An open-source framework for autonomous language agents. *arXiv preprint arXiv:2309.07870*, 2023.

A Case Study Results

Figure 5: Case Study - Task 1: Anomaly Detection

Role	Type	Content																							
User	To Planner	detect anomaly on time_series table from database																							
Planner	Plan	1. instruct CodeInterpreter to pull data from the time_series table in the database 2. confirm the columns to be detected anomalies 3. instruct CodeInterpreter to detect anomalies on the pulled data 4. report the detected anomalies to the user																							
	Current_Plan_Step	1. instruct CodeInterpreter to pull data from the time_series table in the database																							
	To CodeInterpreter	Please pull data from the time_series table in the database																							
CodeInterpreter	Thought	ProgramApe will generate a code snippet to pull data from the time_series table in the database using the sql_pull_data function.																							
	Python	<pre>query = "SELECT * FROM time_series" df, description = sql_pull_data(query) df, description</pre>																							
	Execution_Status	SUCCESS																							
		The execution of the generated python code above has succeeded The result of above Python code after execution is: <table border="1"> <thead> <tr> <th></th> <th>ts</th> <th>val</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>2023-02-01T00:00:00Z</td> <td>67814.0</td> </tr> <tr> <td>1</td> <td>2023-02-01T04:00:00Z</td> <td>84569.0</td> </tr> <tr> <td>..</td> <td>...</td> <td>...</td> </tr> <tr> <td>718</td> <td>2023-05-31T16:00:00Z</td> <td>89912.0</td> </tr> <tr> <td>719</td> <td>2023-05-31T20:00:00Z</td> <td>87249.0</td> </tr> </tbody> </table> [720 rows x 2 columns], 'I have generated a SQL query based on `SELECT * FROM time_series`. The SQL query is SELECT * FROM time_series;. There are 720 rows in the result.		ts	val	0	2023-02-01T00:00:00Z	67814.0	1	2023-02-01T04:00:00Z	84569.0	718	2023-05-31T16:00:00Z	89912.0	719	2023-05-31T20:00:00Z	87249.0					
	ts	val																							
0	2023-02-01T00:00:00Z	67814.0																							
1	2023-02-01T04:00:00Z	84569.0																							
..																							
718	2023-05-31T16:00:00Z	89912.0																							
719	2023-05-31T20:00:00Z	87249.0																							
To Planner	<Information above>																								
Plan	<Plan does not change, not displayed>																								
Current_Plan_Step	2. confirm the columns to be detected anomalies																								
CodeInterpreter	To User	I have pulled the data from the time_series table in the database. The table has the following columns: 'ts' and 'val'. Which column(s) do you want to detect anomalies on?																							
User	To Planner	please use ts and val columns																							
Plan	<Plan does not change, not displayed>																								
Current_Plan_Step	3. instruct CodeInterpreter to detect anomalies on the pulled data																								
To CodeInterpreter	Please detect anomalies on the 'ts' and 'val' columns of the pulled data																								
Thought	ProgramApe will generate a code snippet to detect anomalies on the 'ts' and 'val' columns of the pulled data using the anomaly_detection function.																								
Python	<pre>time_col_name = 'ts' value_col_name = 'val' df_anomalies, anomaly_description = anomaly_detection(df, time_col_name, value_col_name) df_anomalies, anomaly_description</pre>																								
CodeInterpreter	Execution_Status	SUCCESS																							
		The execution of the generated python code above has succeeded The result of above Python code after execution is: <table border="1"> <thead> <tr> <th></th> <th>ts</th> <th>val</th> <th>Is_Anomaly</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>2023-02-01 00:00:00+00:00</td> <td>67814.0</td> <td>False</td> </tr> <tr> <td>1</td> <td>2023-02-01 04:00:00+00:00</td> <td>84569.0</td> <td>False</td> </tr> <tr> <td>..</td> <td>...</td> <td>...</td> <td>...</td> </tr> <tr> <td>718</td> <td>2023-05-31 16:00:00+00:00</td> <td>89912.0</td> <td>False</td> </tr> <tr> <td>719</td> <td>2023-05-31 20:00:00+00:00</td> <td>87249.0</td> <td>False</td> </tr> </tbody> </table> [720 rows x 3 columns], 'There are 11 anomalies in the time series data'		ts	val	Is_Anomaly	0	2023-02-01 00:00:00+00:00	67814.0	False	1	2023-02-01 04:00:00+00:00	84569.0	False	718	2023-05-31 16:00:00+00:00	89912.0	False	719	2023-05-31 20:00:00+00:00	87249.0
	ts	val	Is_Anomaly																						
0	2023-02-01 00:00:00+00:00	67814.0	False																						
1	2023-02-01 04:00:00+00:00	84569.0	False																						
..																						
718	2023-05-31 16:00:00+00:00	89912.0	False																						
719	2023-05-31 20:00:00+00:00	87249.0	False																						
To Planner	<Information above>																								
Plan	<Plan does not change, not displayed>																								
Current_Plan_Step	4. report the detected anomalies to the user																								
To User	I have detected anomalies on the 'ts' and 'val' columns of the pulled data. There are 11 anomalies in the time series data.																								

Figure 6: Case Study - Task 2: Stock Price Forecasting

Role	Type	Content																																										
User	To Planner	use ARIMA model to forecast QQQ in next 7 days																																										
Planner	Plan	1. instruct CodeInterpreter to load QQQ historical data 2. preprocess the data 3. train the ARIMA model 4. forecast QQQ for the next 7 days 5. report the forecasted values to the user																																										
		Current_Plan_Step 1. instruct CodeInterpreter to load QQQ historical data																																										
	To CodeInterpreter	Please load QQQ historical data																																										
	Thought	ProgramApe will generate a code snippet to load QQQ historical data using pandas_datareader library.																																										
CodeInterpreter	Python	import pandas_datareader as pdr import datetime start_date = datetime.datetime.now() - datetime.timedelta(days=365) end_date = datetime.datetime.now() qqq_data = pdr.get_data_yahoo('QQQ', start=start_date, end=end_date) qqq_data																																										
		Execution_Status FAILURE																																										
	Execution_Result	The execution of the generated python code above has failed During execution, the following messages were logged: ----- TypeError Traceback (most recent call last) Cell In[1], line 7 4 start_date = datetime.datetime.now() - datetime.timedelta(days=365) 5 end_date = datetime.datetime.now() ---> 7 qqq_data = pdr.get_data_yahoo('QQQ', start=start_date, end=end_date) 8 qqq_data File \path\to\python\Lib\site-packages\pandas_datareader\data.py:80, in get_data_yahoo(*args, **kwargs) 79 def get_data_yahoo(*args, **kwargs): ---> 80 return YahooDailyReader(*args, **kwargs).read() ... The execution of the previous generated code has failed. If you think you can fix the problem by rewriting the code, please generate code and run it again. Otherwise, please explain the problem to me. <Python> <Execution_Result>																																										
		Thought ProgramApe understands that the execution of the previous round has failed. ProgramApe will attempt to fix the problem by using an alternative method to load QQQ historical data using the yfinance library.																																										
	Python	!pip install yfinance import yfinance as yf import datetime start_date = datetime.datetime.now() - datetime.timedelta(days=365) end_date = datetime.datetime.now() qqq_data = yf.download('QQQ', start=start_date, end=end_date) qqq_data																																										
		Execution_Status SUCCESS																																										
Execution_Result	Execution_Result	The execution of the generated python code above has succeeded The result of above Python code after execution is: <table border="1"> <thead> <tr> <th>Date</th> <th>Open</th> <th>High</th> <th>Low</th> <th>Close</th> <th>Adj Close</th> <th>Volume</th> </tr> </thead> <tbody> <tr> <td>2022-11-28</td> <td>284.899994</td> <td>286.959991</td> <td>281.760010</td> <td>282.709991</td> <td>280.806580</td> <td>38714200</td> </tr> <tr> <td>2022-11-29</td> <td>282.940002</td> <td>283.350006</td> <td>279.170013</td> <td>280.570007</td> <td>278.681061</td> <td>35618900</td> </tr> <tr> <td>...</td> <td>...</td> <td>...</td> <td>...</td> <td>...</td> <td>...</td> <td>...</td> </tr> <tr> <td>2023-11-22</td> <td>390.570007</td> <td>393.070007</td> <td>389.040009</td> <td>390.059998</td> <td>390.059998</td> <td>44121000</td> </tr> <tr> <td>2023-11-24</td> <td>389.649994</td> <td>390.250000</td> <td>388.500000</td> <td>389.510010</td> <td>389.510010</td> <td>15718800</td> </tr> </tbody> </table> 250 rows x 6 columns	Date	Open	High	Low	Close	Adj Close	Volume	2022-11-28	284.899994	286.959991	281.760010	282.709991	280.806580	38714200	2022-11-29	282.940002	283.350006	279.170013	280.570007	278.681061	35618900	2023-11-22	390.570007	393.070007	389.040009	390.059998	390.059998	44121000	2023-11-24	389.649994	390.250000	388.500000	389.510010	389.510010	15718800
Date	Open	High	Low	Close	Adj Close	Volume																																						
2022-11-28	284.899994	286.959991	281.760010	282.709991	280.806580	38714200																																						
2022-11-29	282.940002	283.350006	279.170013	280.570007	278.681061	35618900																																						
...																																						
2023-11-22	390.570007	393.070007	389.040009	390.059998	390.059998	44121000																																						
2023-11-24	389.649994	390.250000	388.500000	389.510010	389.510010	15718800																																						
To Planner <Information above>																																												

Planner	<i>Plan</i>	<Plan does not change, not displayed>
	<i>Current_Plan_Step</i>	2. preprocess the data
	<i>To CodeInterpreter</i>	Please preprocess the QQQ historical data and prepare it for ARIMA model training
CodeInterpreter	<i>Thought</i>	ProgramApe will generate a code snippet to preprocess the QQQ historical data and prepare it for ARIMA model training.
	<i>Python</i>	import pandas as pd # Keep only the 'Close' column qqq_close = qqq_data['Close'] # Resample the data to daily frequency qqq_daily = qqq_close.resample('D').mean() # Fill missing values with the previous day's value qqq_daily_filled = qqq_daily.fillna(method='ffill') qqq_daily_filled
		SUCCESS
		The execution of the generated python code above has succeeded The result of above Python code after execution is: Date 2022-11-28 282.709991 2022-11-29 280.570007 ... 2023-11-23 390.059998 2023-11-24 389.510010 Freq: D, Name: Close, Length: 362, dtype: float64
		<i>To Planner</i>
	<i>Plan</i>	<Plan does not change, not displayed>
	<i>Current_Plan_Step</i>	3. train the ARIMA model
CodeInterpreter	<i>To Planner</i>	Please train the ARIMA model using the preprocessed QQQ historical data
	<i>Thought</i>	ProgramApe will generate a code snippet to train the ARIMA model using the preprocessed QQQ historical data.
	<i>Python</i>	from statsmodels.tsa.arima.model import ARIMA # Fit the ARIMA model model = ARIMA(qqq_daily_filled, order=(1, 1, 1)) model_fit = model.fit() model_fit
		SUCCESS
		The execution of the generated python code above has succeeded The result of above Python code after execution is: <statsmodels.tsa.arima.model.ARIMAResultsWrapper at 0x7f53c83c9040>
		<i>To Planner</i>
	<i>Plan</i>	<Plan does not change, not displayed>
Planner	<i>Current_Plan_Step</i>	4. forecast QQQ for the next 7 days
	<i>To CodeInterpreter</i>	Please use the trained ARIMA model to forecast QQQ for the next 7 days
	<i>Thought</i>	ProgramApe will generate a code snippet to use the trained ARIMA model to forecast QQQ for the next 7 days.
CodeInterpreter	<i>Python</i>	forecast_steps = 7 forecast = model_fit.forecast(steps=forecast_steps) forecast
		SUCCESS
		The execution of the generated python code above has succeeded The result of above Python code after execution is: 2023-11-25 389.557766 2023-11-26 389.530163 2023-11-27 389.546117 2023-11-28 389.536896 2023-11-29 389.542226 2023-11-30 389.539145 2023-12-01 389.540926 Freq: D, Name: predicted_mean, dtype: float64
		<i>To Planner</i>
		<Information above>
	<i>Plan</i>	<Plan does not change, not displayed>
	<i>Current_Plan_Step</i>	5. report the forecasted values to the user
Planner	<i>To User</i>	The ARIMA model has been used to forecast QQQ for the next 7 days. The forecasted values are as follows: 2023-11-25: 389.56 2023-11-26: 389.53 2023-11-27: 389.55 2023-11-28: 389.54 2023-11-29: 389.54 2023-11-30: 389.54 2023-12-01: 389.54

B Planning Example

The following is a planning example for the user query of counting the rows of a CSV file. The example consists of 4 posts:

1. This is the post from the user containing the user query.
2. This is the post from the Planner to the Code Interpreter. The post contains 3 attachments that are the initial plan, the plan (final), and the current step in the plan.
3. This is the post from the Code Interpreter to the Planner on the execution result.
4. This is the post from the Planner to the User, i.e., the response after successfully conducting the query.

These 4 posts consist of a round of conversation between the Planner and the User.

```
1 user_query: count the rows of /home/data.csv
2 post_list:
3 - message: count the rows of /home/data.csv
4   send_from: User
5   send_to: Planner
6   attachment_list:
7     - message: Please load /home/data.csv and count the rows
8       send_from: Planner
9       send_to: CodeInterpreter
10      attachment_list:
11        - type: init_plan
12          content: |-
13            1. load the data file
14            2. count the rows of the loaded data <sequential depend on 1>
15            3. report the result to the user <interactive depend on 2>
16        - type: plan
17          content: |-
18            1. instruct CI to load the file and count the rows
19            2. report the result to the user
20        - type: current_plan_step
21          content: 1. instruct CI to load the file and count the rows
22    - message: Load successfully and there are 100 rows
23      send_from: CodeInterpreter
24      send_to: Planner
25      attachment_list:
26        - message: The file is loaded and there are 100 rows
27          send_from: Planner
28          send_to: User
29          attachment_list:
30            - type: init_plan
31              content: |-
32                1. load the data file
33                2. count the rows of the loaded data <sequential depend on 1>
34                3. report the result to the user <interactive depend on 2>
35            - type: plan
36              content: |-
37                1. instruct CI to load the file and count the rows
38                2. report the result to the user
39            - type: current_plan_step
40              content: 2. report the result to the user
```

C Code Generation Example

The following is a code generation example for the user query of generating 10 random numbers. This example contains 2 posts:

1. This is the post from the user containing the user query.

2. This is the post from the Code Interpreter to the Planner including thoughts, the generated code, and the verification and execution results.

```

1 user_query: generate 10 random numbers
2 post_list:
3 - message: generate 10 random numbers
4   send_from: Planner
5   send_to: CodeInterpreter
6   attachment_list: []
7 - message: The random numbers are 0.2, 0.4, 0.6, ...
8   send_from: CodeInterpreter
9   send_to: Planner
10  attachment_list:
11    - type: thought
12      content: CI will generate 10 random numbers using np.random.
13    - type: python
14      content: |-
15        import numpy as np
16        random_numbers = np.random.rand(10)
17        random_numbers
18    - type: verification
19      content: CORRECT
20    - type: code_error
21      content: No error is detected.
22    - type: execution_status
23      content: SUCCESS
24    - type: execution_result
25      content: The random numbers are 0.2, 0.4, 0.6, ...

```

D Plugin Example

The following is an example of the specification of a plugin named ‘anomaly_detection’. It has 3 input arguments (df, ts_col, and val_col), and 2 return values (df and description).

```

1 name: anomaly_detection
2 description: >-
3   anomaly_detection function identifies anomalies from an input
4   DataFrame of time series. It will add a new column "Is_Anomaly",
5   where each entry will be marked with "True"
6   if the value is an anomaly or "False" otherwise.
7
8 parameters:
9   - name: df
10    type: DataFrame
11    required: true
12    description: >-
13      the input data from which we can identify the anomalies
14      with the 3-sigma algorithm.
15   - name: ts_col
16    type: str
17    required: true
18    description: name of the column that contains the datetime
19   - name: val_col
20    type: str
21    required: true
22    description: name of the column that contains the numeric values.
23
24 returns:
25   - name: df
26    type: DataFrame
27    description: >-
28      This DataFrame extends the input DataFrame with a newly-added
29      column "Is_Anomaly" containing the anomaly detection result.

```

```
30     - name: description
31         type: str
32         description: a string describing the anomaly detection results.
```

The following shows the Python implementation of the anomaly_detection plugin.

```
1 def __call__(self, df: pd.DataFrame, ts_col: str, val_col: str):
2     try:
3         df[ts_col] = pd.to_datetime(df[ts_col])
4     except Exception:
5         print("Time column is not datetime")
6         return
7
8     if not is_numeric_dtype(df[val_col]):
9         try:
10             df[val_col] = df[val_col].astype(float)
11         except ValueError:
12             print("Value column is not numeric")
13             return
14
15     mean, std = df[val_col].mean(), df[val_col].std()
16     cutoff = std * 3
17     l, u = mean - cutoff, mean + cutoff
18     df["Is_Anomaly"] = df[val_col].apply(lambda x: x < l or x > u)
19     anomaly_count = df["Is_Anomaly"].sum()
20     desc = f"There are {anomaly_count} anomalies in the data"
21
22     return df, desc
```