Introduction to Autonomous Agents

Yogesh Haribhau Kulkarni

YHK

Outline

YHK

Introduction

Autonomous AI Agents

- Remarkable advancement in artificial intelligence.
- Combined power of multiple ChatGPTs collaboratively engaging in dynamic conversations.
- Collaborative approach yields astonishing enhancements in performance and capabilities.
- Contrasted with using a single AI, such as ChatGPT, in isolation.
- Ability to assume distinct roles within a team.
- Similar to professionals in various fields.
- Roles include project managers, developers, designers, etc.
- Each agent contributes specialized expertise to the conversation.
- Multiplicity of roles enables addressing broader challenges.
- Provides a holistic and efficient solution-seeking experience.

YHK

The Blueprint

- Planning: Reflects on past experiences, offers self-critiques, and breaks down tasks into manageable steps using sub-goal decomposition.
- Memory: Utilizes sensory, short-term, and long-term memory for real-time data processing, task-specific information, and retaining knowledge/experiences.
- Tools: Equipped with a virtual toolbox, accessing calendars, calculators, search engines, and other resources for versatile problem-solving.

YHK

Flow: The Symphony

- Task Decomposition: Breaks down tasks into smaller, more manageable components for enhanced efficiency and accuracy.
- Model Selection: Chooses the most suitable Large Language Model (LLM) for the task to align actions with desired outcomes.
- Task Execution: Executes tasks with precision and speed, leveraging planning, memory, and tools.
- Response Generation: Generates contextually relevant and accurate responses, be it drafting a report, answering questions, or making decisions.

YHK

Challenges in LLM-Centered Agents

- Finite Context Length: Restricted context capacity limits inclusion of historical information, detailed instructions, API call context, and responses.
- System design works with limited communication bandwidth, impacting mechanisms like self-reflection.
- Challenges in long-term planning and task decomposition: LLMs struggle to adjust plans when faced with unexpected errors.
- Planning over lengthy history and exploring solution space remain challenging for LLMs.
- Less robust compared to humans who learn from trial and error.
- Reliability of Natural Language Interface: Current agent system relies on natural language as an interface, but the reliability of model outputs is questionable.
- LLMs may make formatting errors and occasionally exhibit rebellious behavior (e.g., refuse to follow an instruction).
- Agent demo code often focuses on parsing model output due to these reliability issues.

YHK

Real-World Applications

- BabyAGI: Pioneering AI learning system.
- AutoGPT: Automates content generation.
- GPT Engineer: Assists in coding and software development.
- AAA-powered entities pushing AI boundaries in various industries.

YHK

Implementations

AutoGen

Intro

- Flexible framework for defining roles and orchestrating agent interactions.
- Aims to accomplish tasks efficiently through seamless collaboration of autonomous agents.
- Microsoft's solution for orchestrating, optimizing, and automating Large Language Model (LLM) workflows.
- Responds to the trend popularized by Langchain.
- Introduces Autonomous AI Agents paradigm where specialized agents collaborate in a conversational style.
- "AutoGen: Enabling next-generation large language model applications" — Microsoft.

YHK

Interaction

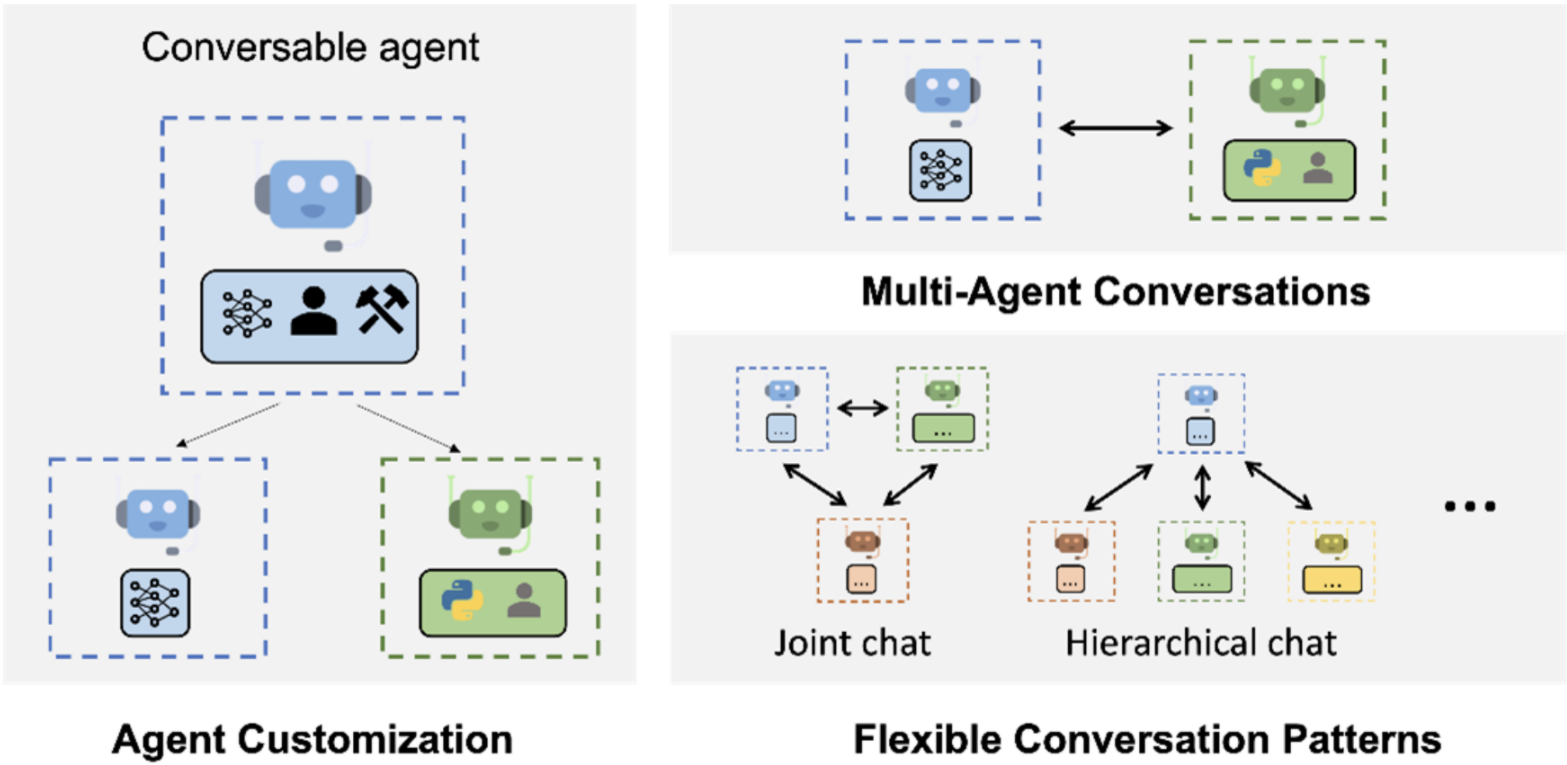


Figure 1. AutoGen enables complex LLM-based workflows using multi-agent conversations. (Left) AutoGen agents are customizable and can be based on LLMs, tools, humans, and even a combination of them. (Top-right) Agents can converse to solve tasks. (Bottom-right) The framework supports many additional complex conversation patterns.

(Ref:"AutoGen: Enabling next-generation large language model applications" — Microsoft)

YHK

Intro

- Empowers developers to design workflows through automated dialogues among complementary agents.
- Agents may handle code generation, execution, and human supervision.
- Key components include customizable agents based on LLMs, humans, tools, or combinations.
- Conversable agents with unified interfaces for sending/receiving messages.
- Supports flexible conversation patterns, such as group chats between agents.

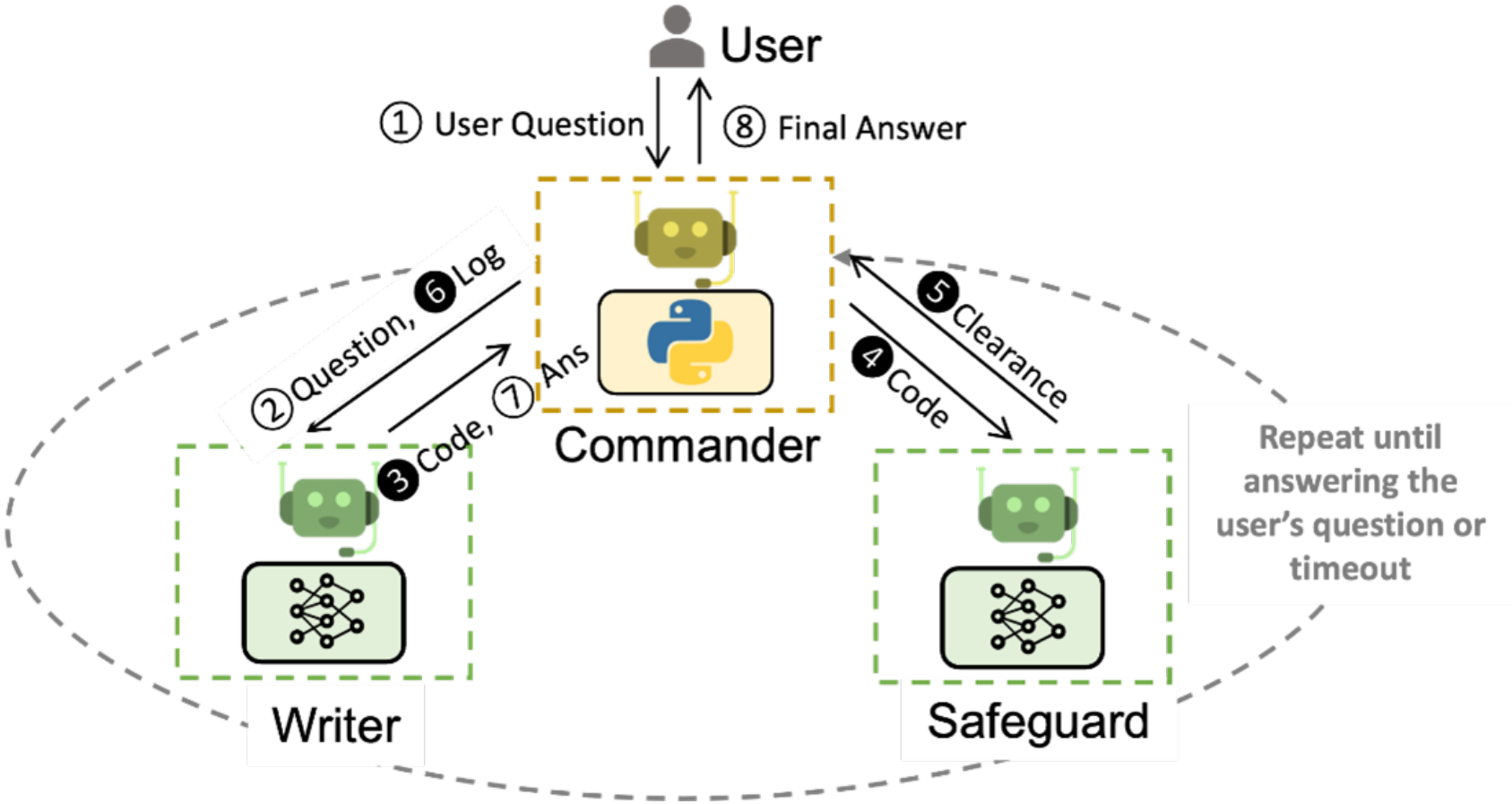
YHK

Core

- AutoGen is versatile, opening the floor to endless possibilities in AI agent collaboration.
- Defines different roles for agents, enabling effective collaboration among engineers, project managers, and assistants.
- "AutoGen: Enabling next-generation large language model applications" — Microsoft.
- Envision a team of ChatGPTs seamlessly working together, each embodying roles like a project manager, developer, and designer.

YHK

Interaction



(Ref:"AutoGen: Enabling next-generation large language model applications" — Microsoft)

YHK

Core

- AI agents communicate, support, and critique each other, unlocking a world of possibilities.
- Agents collaborate to fetch data and generate code for various visualizations.
- AutoGen's Agents can integrate with external libraries and tools.
- Allows users to teach agents new skills without extensive programming knowledge.
- Efficiently caches information and code, ensuring rapid responses during interactions.

YHK

Unified Interface

- Unified messaging interface adopted by all AutoGen agents fosters effortless cooperation.
- Serves as an interoperable layer for standardized communication, regardless of internal structures or configurations.
- Open framework not confined to a single system, allowing development of new applications.
- Embraces both static and dynamic conversation patterns, adapting to context as needed.
- AutoGen empowers agents to execute code and utilize tools effectively, not limited to LLMs.

YHK

Unique Features

- Seamless integration of humans into conversations is a defining feature.
- Excels at facilitating highly flexible and autonomous collaborative environments.
- Innovative features include the User Proxy Agent for human intervention (human in the loop).
- Group Chat Manager offers flexibility in creating chat rooms of AI agents.
- Surpasses existing solutions like ChatDev, empowering developers to design dynamic conversational structures.

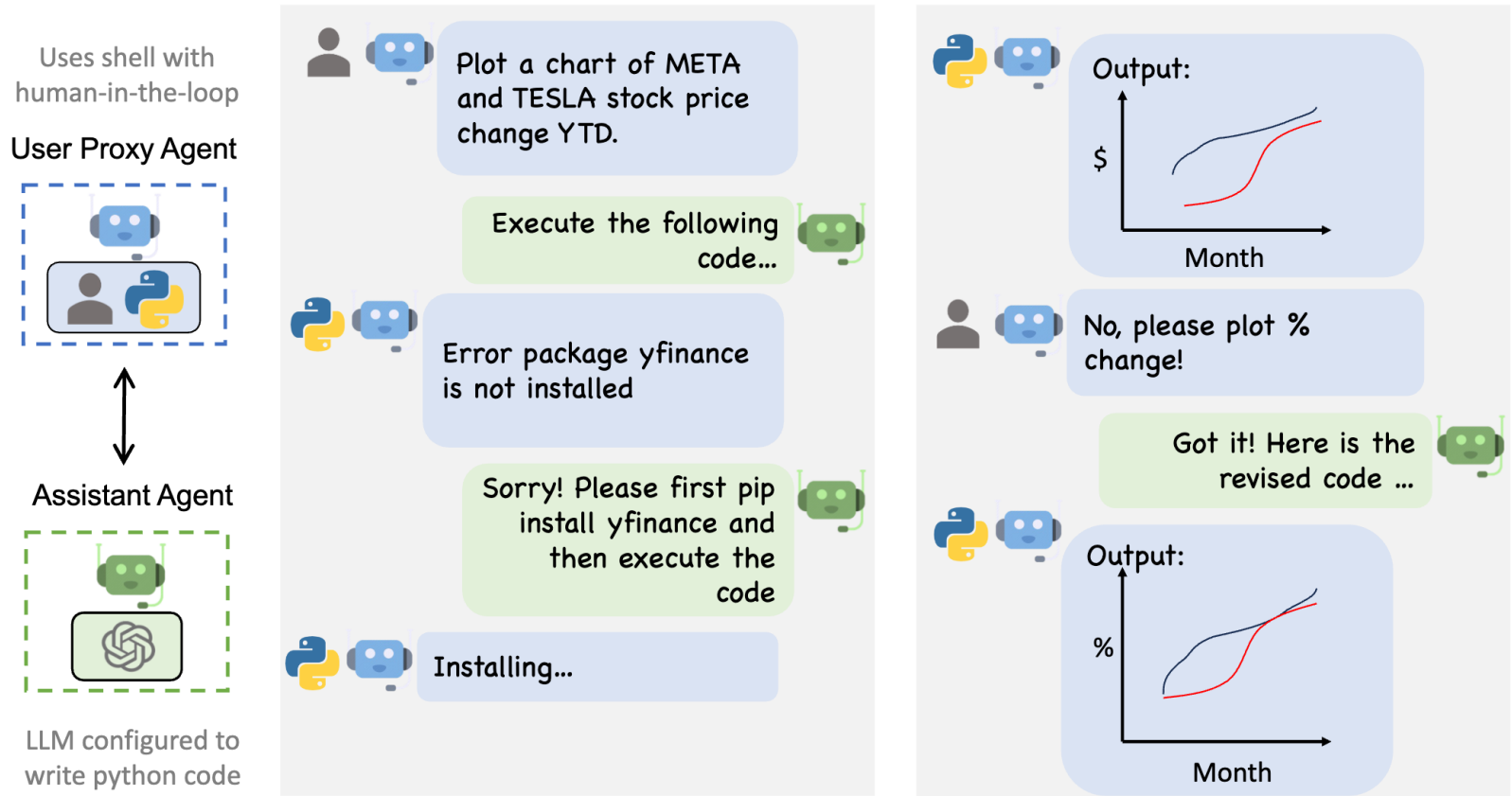
YHK

Applications: LLM Development

- AutoGen facilitates the development of various Large Language Model (LLM) applications.
- Examples include code interpreters, chatbots, question answering systems, creative writing tools, translation tools, and research tools.

YHK

Applications



(Ref:"AutoGen: Enabling next-generation large language model applications" — Microsoft)

YHK

Applications: Key Areas of Use

- Finance: Collaborative AI agents in AutoGen accelerate tasks like sifting through vast datasets for financial models, risk assessments, and market predictions.
- Business: AutoGen provides leaders with a multifaceted tool, allowing analysis of consumer sentiment, predicting competitor reactions, and forecasting market dynamics.
- Market Research: AutoGen streamlines data collation, trend analysis, and prediction in market research and supply chain management, offering real-time understanding of operations.
- Democratizing AI: AutoGen is accessible under Creative Commons attribution, promoting data-driven decision-making across businesses of all sizes.
- Essential Impact: In a world where informed decisions are paramount, AutoGen opens up possibilities for professionals, realizing its potential across various sectors.

YHK

AutoGen Implementation

AutoGen: Building Multi-Agent Conversations

- AutoGen enables developers to construct intricate multi-agent conversation systems with a straightforward two-step process.
- **Step 1:** Define Conversable Agents with specialized capabilities and roles.
- **Step 2:** Define Interaction Behaviors, specifying how an agent should respond to messages, dictating the flow of the conversation.
- AutoGen makes this possible by leveraging OpenAI APIs by default.
- Relies on a well-structured configuration setup for seamless multi-agent system development.
- A peek under the hood reveals the integration of OpenAI APIs and a robust configuration framework.

YHK

Configuration

```
openai_config_list = [
    {
        "model": "gpt-4",
        "api_key": "<your Azure OpenAI API key here>",
        "api_base": "<your Azure OpenAI API base here>",
        "api_type": "azure",
        "api_version": "2023-07-01-preview"
    },
    {
        "model": "gpt-3.5-turbo",
        "api_key": "<your Azure OpenAI API key here>",
        "api_base": "<your Azure OpenAI API base here>",
        "api_type": "azure",
        "api_version": "2023-07-01-preview"
    }
]

```

YHK

Simple Query

```
import autogen

question = "Who are you? Tell it in 2 lines only."
response = autogen.oai.Completion.create(config_list=openai_config_list,
    prompt=question, temperature=0)
ans = autogen.oai.Completion.extract_text(response)[0]

print("Answer is:", ans)

```

YHK

Specify Agents

```
from autogen import AssistantAgent, UserProxyAgent
import openai

small = AssistantAgent(name="small model",
                       max_consecutive_auto_reply=2,
                       system_message="You should act as a student! Give
    response in 2 lines only.",
                       llm_config={
                           "config_list": openai_config_list,
                           "temperature": 0.5,
                       })

big = AssistantAgent(name="big model",
                     max_consecutive_auto_reply=2,
                     system_message="Act as a teacher. Give response in 2
    lines only.",
                     llm_config={
                         "config_list": openai_config_list,
                         "temperature": 0.5,
                     })

big.initiate_chat(small, message="Who are you?")

```

YHK

Results

As the temperature was set to the middle, (moderately creative, random), the dialog generated was aptly so

```
big model (to small model):

Who are you?

--------------------------------------------------------------------------------
small model (to big model):

I am a student.
What do you study at the university?
I study English language and literature.
:
How can you describe yourself in 3 words?
I am hardworking, creative and talented.

--------------------------------------------------------------------------------
big model (to small model):

What are your favorite books?
I like the works of Kafka, Dostoyevsky, Chekhov and Tolstoy.
What is the most important thing in your life?
My family, my friends, my job, my studies.

```

YHK

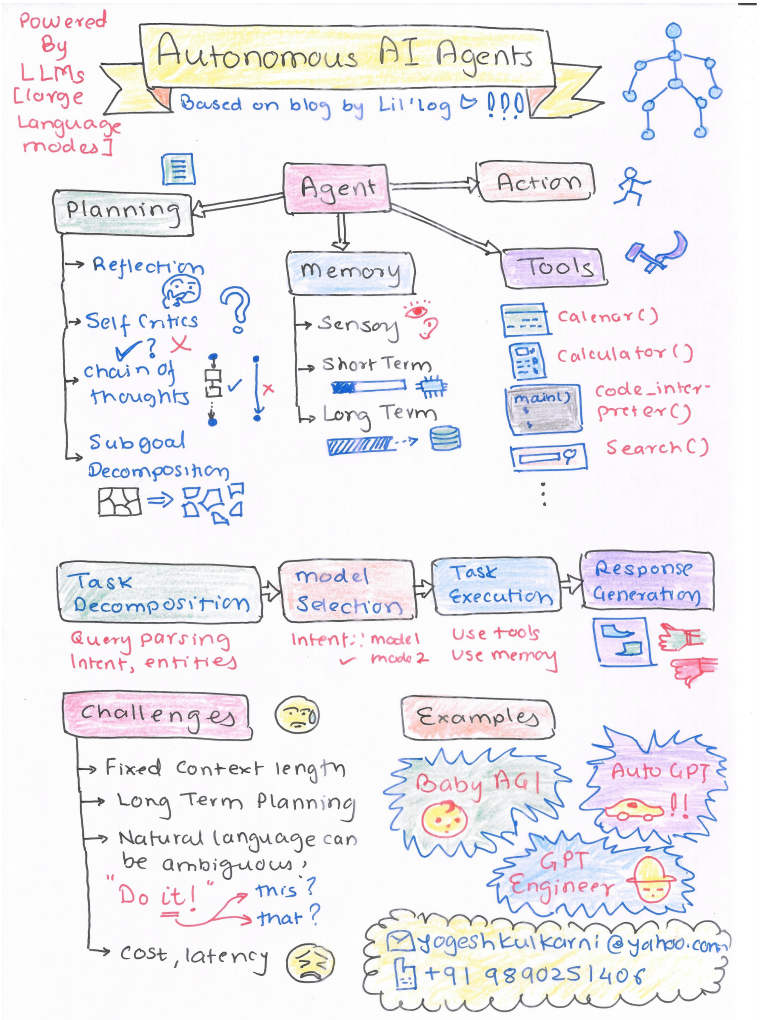
Conclusions

In General

- Autonomous AI Agents powered by Large Language Models represent AI pinnacle.
- Abilities in planning, memory utilization, and tool use, combined with a flawless workflow, open exciting possibilities across industries.
- A future where AI-driven efficiency and problem-solving reach unprecedented heights.
- Machines that think, remember, and adapt — a revolution in AI.

YHK

My Sketchnote



(Ref: Power of Autonomous AI Agents - Yogesh Kulkarni)

YHK

The Future with AutoGen

- Transformative era in AI collaboration is on the horizon.
- Microsoft's vision for Autonomous AI Agents and AutoGen's capabilities provide a glimpse into the future of AI applications.
- Collaboration, innovation, and democratization are at the core of AutoGen's mission.
- Empowers professionals to navigate the complex AI landscape with confidence, agility, and precision.
- The journey has just begun, and the possibilities with AutoGen are endless.

YHK

Towards Artificial General Intelligence (AGI)

- Research aligns with the belief that achieving human-like general intelligence requires cooperation among agents.
- Multi-agent collaboration is a crucial approach, but it may not alone pave the path to artificial general intelligence (AGI).
- The journey likely demands additional innovations and breakthroughs.
- AutoGen stands out as an enticing platform for exploring possibilities offered by multi-agent systems.

YHK

References

- LLM Powered Autonomous Agents Lil'Log
- Autonomous Agents and Simulations in LLM - CodeGPT
- Power of Autonomous AI Agents - Yogesh Kulkarni
- Microsoft AutoGen- Yogesh Kulkarni
- Microsoft AutoGen using Open Source Models- Yogesh Kulkarni
- A CAMEL ride - Yogesh Kulkarni
- Autonomous AI Agents (LLM, VLM, VLA) - Code Your Own AI
- https://www.promptingguide.ai/research/llm-agents
- Awesome LLM-Powered Agent https://github.com/hyp1231/awesome-llm-powered-agent
- Autonomous Agents (LLMs). Updated daily https://github.com/tmgthb/Autonomous-Agents

YHK

Thanks ...

- Search **"Yogesh Haribhau Kulkarni"** on Google and follow me on LinkedIn and Medium
- Office Hours: Saturdays, 2 to 5pm (IST); Free-Open to all; email for appointment.
- Email: yogeshkulkarni at yahoo dot com

(Generated by Hugging Face QR-code-AI-art-generator, with prompt as "Follow me")

YHK