Designing modern chatbots leveraging Large Language Models and the LangChain ecosystem

Candidate:
Gianfranco Demarco

Supervisor:
Dr. Gennaro Vessio
Research Laboratory:
CILAB

University of Bari Aldo Moro
April 17, 2024

Why chatbots?

Chatbots are artificial intelligence programs that use **Natural Language Processing (NLP)** to communicate in human language with users

Employed to replace human operators in:

1. entertainment
2. education
3. information retrieval
4. e-commerce
5. business

Why chatbots?

However, even modern chatbots such as ChatGPT struggle with **complex conversations** and dealing with **structured data**, because they are **stateless** and only rely on conversation history.

Chatbots technologies

Different approaches to build chatbot systems have been explored:

1. Pattern matching
   - rules
   - templates
2. Machine Learning
   - Intent classification
   - Entity extraction
3. **Large Language Models**

Large Language Models

Large Language Models (LLMs) are language models, primarily based on the Transformer architecture, that contain >10B parameters

LLMs show **emergent abilities**:

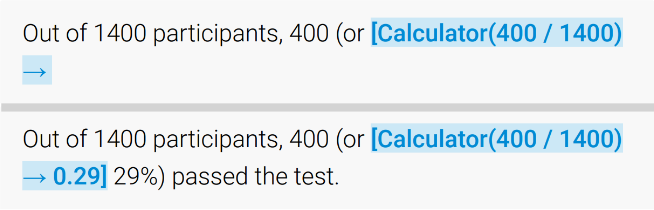
1. few-shot prompting
2. augmented prompting strategies
    - chain-of-thought
    - instruction following
    - program execution

⟶ interact with the external environment through **tools**

Tool calling

LLMs can interact with **external tools**:

- the LLM generates a specific sequence of tokens signaling a tool call
- the program interrupts decoding and executes the tool call
- the result is passed back into the LLM and the decoding continues

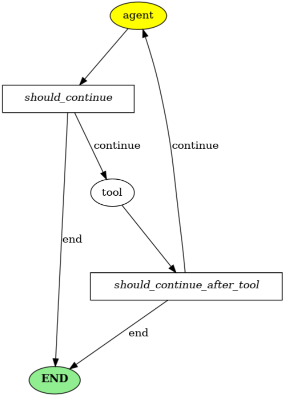


Out of 1400 participants, 400 (or **[Calculator(400 / 1400) →**

Out of 1400 participants, 400 (or **[Calculator(400 / 1400) → 0.29]** 29%) passed the test.

LangChain and LangGraph

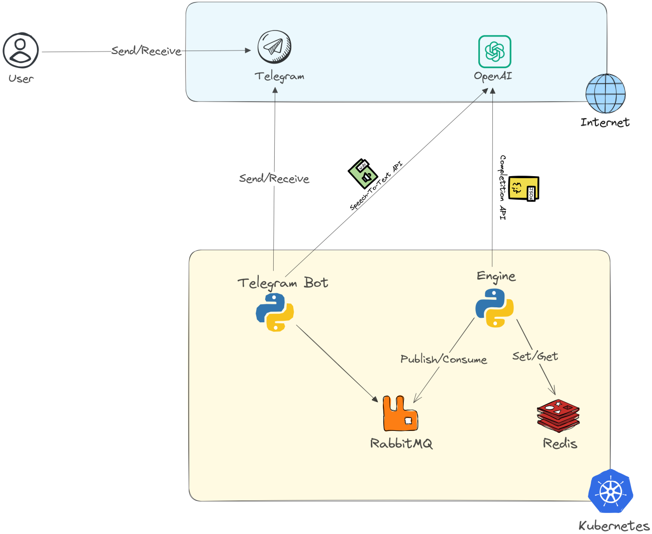
LangChain is a framework for developing applications powered by LLMs. **LangGraph** is a library for building stateful applications with LLMs, represented as graphs.



Aims and Objectives of the thesis

1. Build a complete chatbot system, named WizardAI, using modern technologies such as LLMs and LangChain
2. Introduce a new class of tools (FormTools) as an extension to LangChain for *conversational forms*
    - data acquisition forms through natural language
3. Evaluate FormTools vs standard LangChain tools

System Architecture



Basic Conversation Flow

The conversational engine of WizardAI is implemented based on **LangChain** and **LangGraph**.

1. The history of the conversation is retrieved and composed with the user's current input to get the final model input
2. the OpenAI completion API is called
3. the model outcome is checked
    - textual answer
    - error
    - tool

Available Tools

1. **GoogleCalendarCreator**: create events on Google Calendar
2. **GoogleCalendarRetriever**: retrieve events from Google Calendar
3. **GmailRetriever**: retrieve emails from Gmail
4. **GmailSender**: send emails with Gmail
5. **GoogleSearch**: search on Google
6. **PythonCodeInterpreter**: execute code
7. **OnlinePurchase**: simulate a purchase

Example Conversation #1

User: what is the current price of bitcoin

WizardAI: The current price of Bitcoin is 60,397.13 EUR.

User: what about in dollars?

WizardAI: The current price of Bitcoin in USD is $65,613.40.

User: and if it gains 12%?

WizardAI If Bitcoin gains 12%, the price would be $73,487.01

The system uses the GoogleSearch and CodeInterpreter tools to answer user's questions.

Example Conversation #2

User: I want to create an event called "Idea wear use"

WizardAI: The event "Idea wear use" has been created successfully. It is scheduled for today from 9:00 AM to 10:30 AM.

The system hallucinates input data, causing unwanted side-effects

Conversational forms and FormTools

- Guide the user toward the completion of the action
- Persist the data instead of relying only on the history
- Validate the data and ask follow-up questions
- Ask for confirmation before executing actions

Conversational forms and FormTools

FormTools are *stateful:*

- **inactive**:
  - no FormTool has been activated
  - the conversation follows the normal flow
- **active:**
  - the FormTool has been activated
  - the agent guides the user toward completion
  - other FormTools are hidden
- **filled:**
  - all of the data has been acquired
  - the agent asks for confirmation

The state information and the persisted data guide the agent using custom prompts.

Example Conversation #3 - FormTools

User:	I want to buy shoes.
WizardAI:	Great choice! How many pairs of shoes would you like to purchase?
User:	I would like to purchase 8 pairs of shoes.
WizardAI:	Where would you like the shoes to be shipped? Could you please provide the region for the shipping address?
User:	The region for the shipping address is Toscana.
WizardAI:	Could you please provide the province for the shipping address in Toscana?
User:	The province for the shipping address in Toscana is Pisa.

Example Conversation #3 - FormTools

WizardAI: Thank you for providing the shipping region and province. Now, could you please provide the full address where you would like the shoes to be shipped?

User: 245 Tina Estate Suite 372, New Christinaland, AR 28256

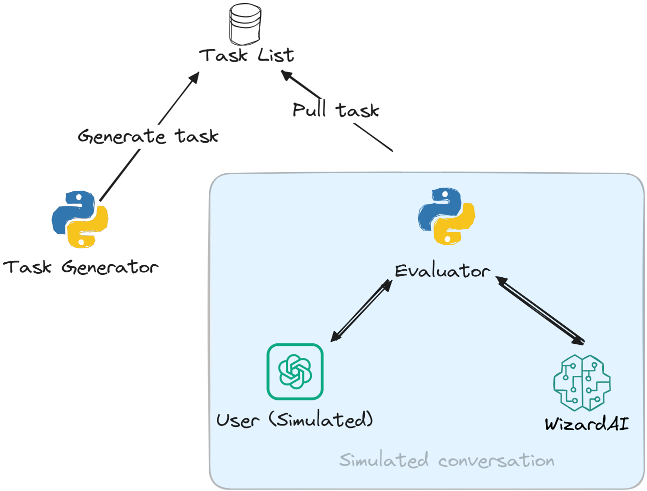
WizardAI: Here is the information for your purchase *[omitted]*. Please confirm if the details are correct so we can proceed with the purchase.

User: Yes, the details are correct. Please proceed with the purchase.

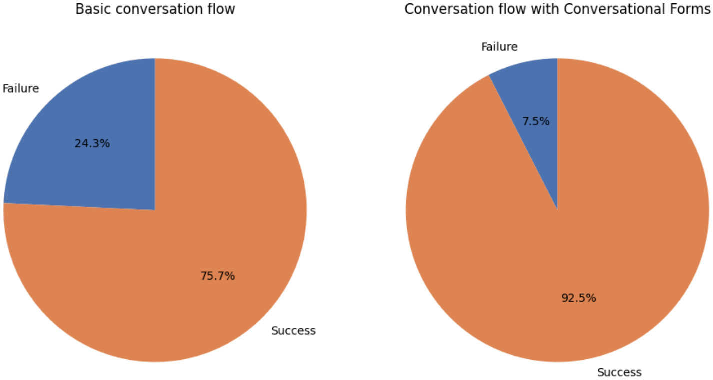
WizardAI: You ordered has been registered. Thank you!

The system is able to guide the user through complex conversations

Evaluation Framework



Results



- Overall success rate goes from 75.7% to 92.5%
- Success rate for OnlinePurchase tool (complex conversational form) goes from 55% to 96.25%

Future works

- Multi-LLM support
- Implement more tools
- Refine prompts and conversation flow
- Extend evaluation

Thank you for your attention!