

Plugins and Tools



גלעד מרקמן
פרויקט ב- Github

Plugins / Tools

- הגדרה - כלים במודלים של בינה מלאכותית הם הרחבות חיצוניות שהמודל יכול לקרוא להם כדי לבצע פעולת עזר.
 - דוגמאות: חיפוש באינטרנט, גישה למסד נתונים, שימוש במחשבוניס ועוד.
- המודל רק "מנבא טקסט", אינו מחובר לעולם החיצוני, והידע שלו אינו עדכני. הכלים נותנים למודל כוח ביצועי:
 - להביא מידע עדכני (מהאינטרנט או מבסיסי מידע)
 - לבצע פעולות מדוייקות (חישוב או שליפת נתונים).
 - לעשות אינטגרציה עם מערכות אמיתיות (לוח שנה, דואר אלקטרוני, מערכות חיצוניות).

החשיבות של הכלים

- הכלים הופכים את המודל מ"מחולל תשובות" ל"עוזר חכם" שמבצע משימות.
- הכלים משפרים את האמינות של המודל כך שייתן תשובות על סמך מידע עדכני ורלוונטי, ולא ינחש תשובות.
- הכלים מאפשרים לפתח אפליקציות מתקדמות, כגון: צ'אטבוט שמזמין טיסות, צאט שעונה לשאלות על תיק רפואי של חולה, וכד'.

דוגמה למגבלות המודלים

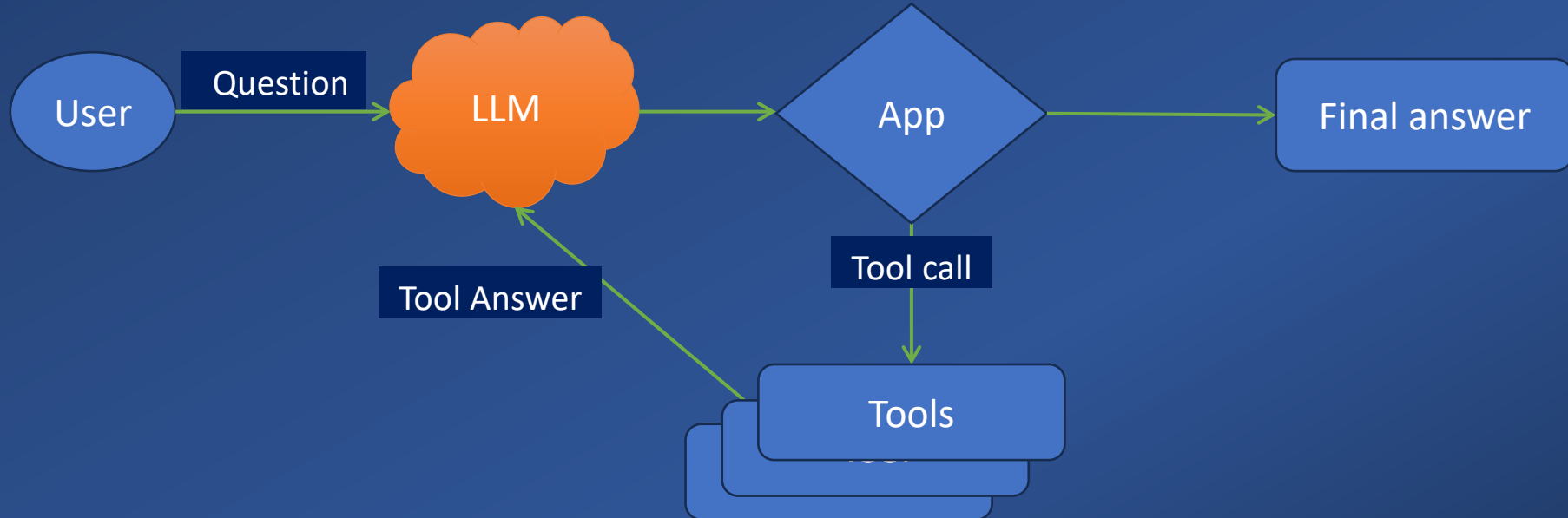
- להלן שיחה עם מודל gpt-4.1-mini המלמדת על מגבלות המודלים:

```
>> what is the date today ?  
Today's date is April 27, 2024.  
>> How old is the state of Israel ?  
The state of Israel was established on May 14, 1948. As of today, April 27, 2024, I srael is 75 years old and will turn 76 in a few weeks.  
>> Who is Gilad Markman from Israel ?  
As of my latest information, there is no widely known or publicly prominent individual named Gilad Markman from Israel. If you have more context or specific details about him, such as his profession or field of activity, please provide them, and I can try to assist you further. Otherwise, he may be a private individual without significant public presence.  
>> who is the president of USA ?  
As of April 27, 2024, the President of the United States is Joe Biden.  
>>
```

- כפי שניתן לראות, המודל אומן על מידע נכון ליום 27/4/2024 כך שהתשובות שלו אינן עדכניות.
- המודל אומן על בסיס מידע עצום אך עדיין מוגבל. על כן, ישנן שאלות שהוא אינו יכול לענות.

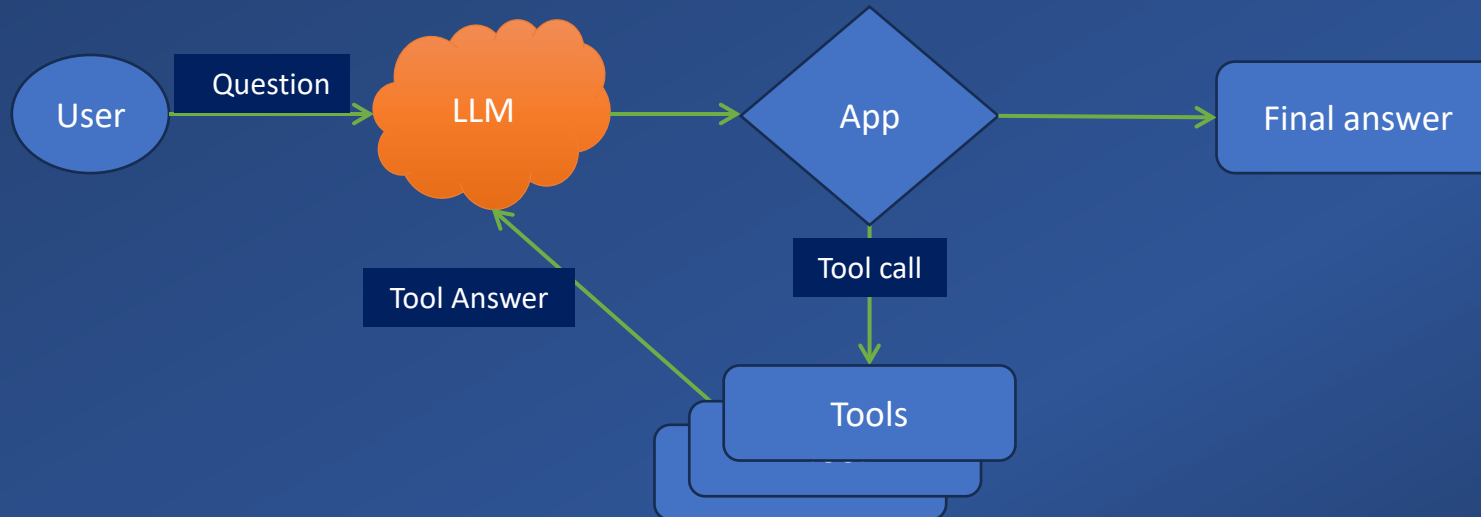
כלים Tools

- כלים הם פעולות שהמודל יכול להפעיל אותם.
- המודל מקבל שאלה ומחליט אם להחזיר תשובה סופית או לבקש מהאפליקציה להפעיל כלי. אם מופעל כלי התשובה חוזרת למודל אשר נותן את התשובה הסופית (אם מבקש הפעלת כלי נוסף).



Output structure

- כדי שהאפליקציה תוכל להחליט על סמך תשובת המודל האם צריך להפעיל כלי מסויים ומהם הפרמטרים להעביר לכלי, התשובה של המודל חייבת להיות במבנה ידוע וקבוע מראש.
- המבנה המקובל להחזרת תשובות בטקסט נקרא JSON.



JSON (JavaScript Object Notation)

- פורמט קל לקריאה ולכתיבה לאחסון והעברת נתונים.
- מבוסס על זוגות של **מפתח-ערך** (key-value).
- נתמך ברוב שפות התכנות ונפוץ מאוד בשימוש באינטרנט.
- אתרי האינטרנט מחזירים את המידע בפורמט של JSON

```
string system = ""  
    Always reply with JSON only:  
    {  
        "Thought": "why you chose the action",  
        "Action": "GetDate" or "FinalAnswer",  
        "Input": "" // empty for GetDate, or the final answer text for FinalAnswer  
    }
```

המרת JSON לאובייקטים

- אחד היתרונות של JSON הוא האפשרות להמיר את הטקסט לאובייקט בשפת תכנון (הדבר נכון בכל שפת התכנות לרבות C#), ולהפך.

- לדוגמה, המרת התשובה של מודל הבינה המלאכותית לאובייקט במקרה שלנו נעשה כך:

```
public class AgentStep
{
    public string Thought { get; set; }
    public string Action { get; set; }
    public string Input { get; set; }
}
```

- הגדרת המחלקה.

```
var stepObj = JsonSerializer.Deserialize<AgentStep>(reply.Content);
```

- המרת ה JSON לאובייקט:

```
string system = ""
Always reply with JSON only:
{
    "Thought": "why you chose the action",
    "Action": "GetDate" or "FinalAnswer",
    "Input": "" // empty for GetDate, or the final answer text for FinalAnswer
}
```

```
if (stepObj.Action == "GetDate")
```

- שימוש באובייקט:

שימוש בכלי – תאריך היום

- נדגים את השימוש בכלים באמצעות כלי פשוט המחזיר את התאריך הנוכחי.
- הכלי – פונקציה ב C# המחזירה את תאריך היום.
- System Prompt: מבהיר למודל הבינה המלאכותית כי עליו להחזיר תשובה תמיד במבנה JSON קבוע. אם זקוק להפעלת הכלי עליו לציין זאת בצורה קבועה מראש, אחרת יחזיר את התשובה הסופית.

```
string system = ""  
Always reply with JSON only:  
{  
  "Thought": "why you chose the action",  
  "Action": "GetDate" or "FinalAnswer",  
  "Input": "" // empty for GetDate, or the final answer text for FinalAnswer  
}  
  
If you need today's date/day to answer, set Action="GetDate" and leave Input empty.  
If you can answer without it, set Action="FinalAnswer" and put the full answer in Input.  
"";
```

שימוש בכלי – תאריך היום

```
// First model reply
var reply = await chatService.GetChatMessageContentAsync(history);
var stepObj = JsonSerializer.Deserialize<AgentStep>(reply.Content);

if (stepObj.Action == "GetDate")
{
    string result = DateTool.GetDate();

    // Give result back to model
    history.AddAssistantMessage(reply.Content);
    history.AddAssistantMessage("[TOOL] GetDate => " + result);
    history.AddUserMessage("Now return FinalAnswer with the result.");

    // Ask model again for final answer
    var finalReply = await chatService.GetChatMessageContentAsync(history);
    var finalStep = JsonSerializer.Deserialize<AgentStep>(finalReply.Content);

    Console.WriteLine(finalStep.Input);
}
else if (stepObj.Action == "FinalAnswer")
{
    Console.WriteLine(stepObj.Input);
}
```

- קריאה למודל הבינה והמרת התשובה מ JSON לאובייקט.
- אם המודל ביקש לקבל תאריך – נקרא לפעולה שמביאה לנו את התאריך, נוסיף אותו להסטוריה, ונקרא שוב למודל הפעם עם התאריך הנוכחי.
- המודל ייתן הפעם תשובה סופית שכן יש לו את התאריך הסופי.

הדגמות

- Plugin1.cs – שימוש בכלי המחזיר תאריך נוכחי.
- Plugin2.cs – שימוש במספר כלים (תאריך ושעה) – לולאת ReAct.
- Plugin3.cs - רישום כלים ב kernel. שימוש אוטומטי בכלים.
- Plugin4.cs – רישום כלים ב Kernel – ללא Stream לצורכי הדגמה של ההיסטוריה.
- Plugin5.cs – שימוש בכלים המקבלים פרמטרים (add(a, b)).

•

כלי גלישה באינטרנט

- המידע של המודלים מוגבל לתאריך בו הסתיים האימון שלהם.
- על מנת להרחיב את בסיס הידע של המודלים פותח הכלי Tavily שמאפשר למודלים לקבל מידע מהאינטרנט.
- אם המודל מחליט כי הוא זקוק למידע מהאנטרנט הוא קורא לכלי עם מילות חיפוש, והכלי מחזיר את תוצאות החיפוש אותם מחזירים למודל לתשובה סופית.
- לצורך שימוש ב Tavily עלינו לגלוש לאתר, לפתוח חשבון ולקבל API.
[אתר tavily](https://tavily.com)
- SK כולל כלי מוכן לשימוש ב Tavily, כפי שמודגם בקוד.

כלי גלישה באינטרנט

- על מנת להשתמש בכלי Tavily המאפשר חיפוש באינטרנט עלינו:
 - לייבא את הספריות הנדרשות.
 - להגדיר Plugin מתאים ולרשום אותו ב kernel.
 - להגדיר שימוש בכלים אוטומטי.
- המודל ישתמש בחיפוש באינטרנט אם יחשוב שהוא זקוק לכך.

```
using Microsoft.SemanticKernel.Plugins.Web.Tavily;  
using Microsoft.SemanticKernel.Data;    // TavilyTextSearchOptions
```

```
// Add Tavily as a plugin named "Web" with a Search function  
var tavily = new TavilyTextSearch(  
    apiKey: TAVILY_API_KEY,  
    options: new TavilyTextSearchOptions { SearchDepth = TavilySearchDepth.Advanced });  
builder.Plugins.Add(tavily.CreateWithGetTextSearchResults("Tavily"));
```

```
_settings = new OpenAIPromptExecutionSettings  
{  
    FunctionChoiceBehavior = FunctionChoiceBehavior.Auto()  
};
```