AI作為學習助理

AI 作為學習助理（II）

從 Prompt 到 Context、Harness 與 Loop Engineering，打造可持續進步的個步的個人學習系統

王昭能

亞洲大學 生物資訊與醫學工程學系 教授

> 不只是「會問 AI」，而是能設計一套讓自己持續進步的學習系統。

問題意識

AI 幫你完成作業，還是幫你完成學習？

AI 代工模式

幫我寫完整報告

幫我解完所有題目

幫我摘要所有內容

追求一次完成

AI 學習助理模式

協助我找出論證漏洞

先給我最小提示

幫我設計主動回想題目

追求持續修正與能力累積

如果明天不能使用 AI，你是否還能解釋、推理、應用與辯護這份成果？

今天的核心主張

AI 的價值不是讓你更快交作業，而是讓你有更更多次高品質的理解、練習、回饋與修正。

理解 → 嘗試 → 回饋 → 修訂 → 驗證 → 遷移

架構總覽

從一句提示詞，到一個學習系統

Prompt ⊂ Context ⊂ Harness ⊂ Loop

01 Prompt

我要如何指令 AI？

讓 AI 知道要做什麼

02 Context

AI 需要知道什麼背景？

讓回應貼近任務與學習者

03 Harness

AI 在什麼規則與工具下下工作？

讓過程安全、可控、可查核

04 Loop

如何反覆練習與修正？

讓能力真正累積與收斂

Prompt Engineering

不是把問題問得很長，而是把任務講得清楚

角色 + 任務 + 限制 + 互動方式 + 成功標準

角色

AI 應以何種觀點協助我？

「你是一位統計學學習教練」

任務

我要完成哪種學習任務？

「協助我理解 p-value」

限制

AI 不可以直接做什麼？

「不要一開始就給完整答案」

互動

希望如何來回？

「先問我三個診斷問題」

成功標準

怎樣算我真的學會？

「我能用自己的話解釋並應用」

Prompt Engineering

從「幫我做」改成「幫我學」

低品質提示詞	高品質學習提示詞
幫我解釋 overfitting	先問我三個問題診斷我對 overfitting 的理解；再用醫療 AI 與考試準備各舉一例。不要直接給完整答案，最後請我用自己的話解釋。
幫我寫一篇 AI 醫療報告	依我的大綱與 rubric，找出論證跳躍、缺乏證據與未定義的概念；不要代寫全文，列出最優先要修訂的三項。
幫我整理這篇論文	先產生五個讀完應能回答的問題；我回答後，再比較我的理解與論文內容，指出遺漏與錯誤。

可直接複製

萬用「AI 學習教練」提示詞

你是我的學習教練，不是代答工具。我正在學習【主題】，目前程度是【先備知識】，目標是在【時間】內達到【可觀察的學習成果】。

請先用 2–3 個問題診斷我的理解，不要直接提供完整答案。我回答後，請指出：我已理解的部分、我推論跳躍的部分、我需要補強的最重要概念。

接著只提供最小必要提示，讓我自行完成推理。最後給我一題不同情境的練習題，並要求我用自己的話總結。

若涉及數據、文獻、引用或事實，請標記所有需要我自行查證之處。

Context Engineering

AI 回答不準，常常不是模型不夠強

回應品質 ≈ Prompt + Context + 驗證機制

> 「幫我改善這份簡報。」

Context 的重點不是把所有資料貼進去，而是提供真正會影響判斷的資訊。

AI 其實不知道——

- **目標是招生、教學、研究提案還是**產學簡報？
- **聽眾是高中生、學生、教師、企業或評審？**
- **可用時間是 5 分鐘、20 分鐘還是 40 分鐘？**
- **目前的**內容與素材是什麼？
- **成功條件是理解度、**說服力還是視覺效果？

Context Engineering

提供給 AI 的 Context，至少包含六件事

01

任務目標

撰寫 1,200 字文獻評論

02

學習者背景

已學過基礎統計、未學過貝氏推論

03

受眾與情境

大二學生、10 分鐘課堂報告

04

可用資料

指定教材、論文、課堂投影片

05

約束條件

不可虛構引用、不代寫全文

06

成功標準

能比較方法、提出限制與案例

Context 範例：論文閱讀

把「摘要論文」改為「建立批判性閱讀對話」

低 Context

幫我摘要這篇論文。

學生停在「消費摘要」，無法判斷方法是否適用於自己的資料。

高 Context

我是生醫資訊研究所學生，正在閱讀單細胞 RNA 定序資料整合的論文。目標不是取得摘要，而是評估此方法能否應用於我的癌症資料。

請只根據我提供的論文內容回答，沒有證據時明確標示「論文未說明」。請分析：研究問題與資料來源、方法的核心假設、評估指標與可能偏誤、可遷移條件、我應追問作者的三個問題。

最後不要給結論，而是要求我先提出自己的方法評估。

Harness Engineering

不是讓 AI 更自由，而是讓 AI 更可靠

```
Agent = Model + Harness
```

Harness 決定 AI 能接觸什麼、如何執行，以及如何被監督。

系統規則與角色設定	指定教材與知識來源
檢索、計算、程式與搜尋工具	權限與隱私保護機制
產出格式與評分規準	事實查核與人工審核關卡
操作紀錄與版本控制	反思歷程與學習檔案

Harness Engineering

每一門課的最小可行學習 Harness

元件	課程中的具體做法	學習效益
指定資料庫	教材、講義、指定論文、可信資料庫	降低錯誤與來源混亂
任務模板	報告、讀書筆記、專題、反思格式	提高產出一致性
Rubric	正確性、證據、論證、表達、反思	使回饋可操作
查核規則	引文、數字、事實、程式碼必須驗證	建立 AI 素養
揭露規則	說明使用工具、目的與範圍	維護學術誠信
學習紀錄	初稿、AI 回饋、修訂稿、反思	評量真實學習歷程

Harness Engineering

誰負責設計 AI 學習環境？

教師設計

說明課程是否允許使用 AI

提供可使用的教材與資料範圍

設計需要思辨與遷移的任務

提供 rubric 與評量標準

設定個資、機密與倫理邊界

學生負責

依規範揭露 AI 使用方式

不使用虛構或未查核的資料

保留原始想法與修訂軌跡

能說明並辯護自己的成果

不上傳敏感或未公開資料

教育 AI 的治理重點不只是導入工具，也包括公平近用、資料保護、透明性、偏誤控制與教師專業自主。

Loop Engineering

從一次問答，到會反覆運轉的學習循環

設計一個會持續「做、看、改、驗證」的流程，並定義何時停止。

01 Plan

規劃

定義今天要學會的具體能力

02 Attempt

嘗試

先自己作答、寫作或解題

03 Feedback

回饋

AI 指出錯誤、迷思與缺口

04 Revise

修訂

依回饋與 rubric 改寫作品

05 Verify

驗證

變式題、查證、口頭說明

Loop Engineering

學生每天可以使用的 AI 學習循環

階段	學生要做什麼	AI 可以做什麼
1 規劃	定義今天要學會的具體能力	協助拆解目標與安排任務
2 嘗試	先自行回答、寫作、解題或畫圖	不直接代答，等待學生輸入
3 診斷	提交思路、答案或草稿	找出錯誤、迷思與缺口
4 回饋	讀取回饋並提出追問	提供最小提示、反例與釐清
5 修訂	修訂自己的答案或作品	依 rubric 再次檢視
6 驗證	查證資料、完成變式題或口頭說明	出新題、扮演評審或反方
7 反思	記錄自己真正學到什麼	協助產生反思問題

案例

用 AI 閱讀一篇生醫資訊論文

階段	學生任務	AI 學習助理任務
規劃	寫下本篇想回答的三個研究問題	協助確認問題是否具體
初讀	自行畫出研究架構與方法流程	不做摘要，只提出澄清問題
解釋	用自己的話說明假設與方法	指出概念錯誤與遺漏
批判	列出方法限制與潛在偏誤	扮演 reviewer 提出反駁
驗證	回到原文確認證據與段落位置	要求標示文中依據
產出與反思	撰寫 300 字 critical appraisal 與理解差異	依 rubric 提供修訂建議

Loop Engineering

什麼時候才算「真的學會」？

~~以「AI 已經給出答案」作為停止條件~~

以「我已能在新情境中獨立完成任務」作為停止條件

四種可衡量的停止條件

不看 AI 回答，正確用自己的話解釋概念

完成不同情境的變式題或實作任務

能說明方法、證據、限制與不確定性

依 rubric 修訂到預定水準並解釋修訂理由

三分鐘活動

請把「幫我做」改成「幫我學」

原始提示詞

> 幫我整理這篇文章，並告訴我考試重點。

改寫後與同組交換，互相檢查學習責任是否還留在自己身上。

依六個欄位改寫

我的學習主題是什麼？

我目前的程度與常見困難是什麼？

AI 需要讀哪些資料？

AI 不能直接替我做什麼？

AI 應如何提問或回饋？

我要如何證明自己真的學會？

責任與倫理

AI 可用，但責任不能外包

01

查核

數字、引用、事實、研究結論與程式碼都要驗證

02

揭露

依課程或研究規範說明工具、範圍與用途

03

保護

不輸入個資、病歷、未公開資料或他人作品

04

負責

只提交自己能說明、辯護與修訂的內容

結語

從使用工具，到設計自己的學習系統

Prompt

我如何清楚提出需求？

Context

我如何提供完整且有用的脈絡？

Harness

我如何建立資料、規則與查核邊界？

Loop

我如何在回饋與修訂中持續進步？

> AI 不應替你縮短思考，而應幫你設計一條更有品質、更能累積能力的思考路徑。