

人工智能的技术脉络

学习、推理、行动与科学发现

第一讲 | 2026年技术全景与四方向应用入口

学习

推理

行动

验证

发现

第一讲 | 本科三年级

量子 · 数学 · 自然科学 · 工程
2026年9月7日

理解前沿能力的来源，找到本专业可以验证的算法入口。

2026年的前沿：模型能力与系统能力共同增长

以截至2026年9月7日可核验的公开成果为例；产品公告与学术证据分别判断。

01

推理与计算

GPT-6 Astra / Gemini
复杂推理与代码执行
搜索和验证预算

02

多模态与生成

文本、图像与序列
预测或构造候选对象
表示与训练目标

03

智能体与工具

Claude / DeepSeek
多步调用软件与工具
反馈、状态与权限

04

科学专用模型

AlphaFold
AlphaQubit
领域数据与验证器
专业任务的约束

发展主线：可学习的表示 + 可扩展的计算 + 可核验的反馈。

读懂一项AI进展，先区分四种证据

一个成功案例、一个高分模型与一个可运行系统，回答的是不同问题。



形式证明、物理实验与工程运行需要各自适用的证据。

本讲顺序：技术脉络 → 计算机制 → 应用变化 → 科学前沿 → 课程入口。

人工智能的历史，是知识与反馈进入计算的历史

符号、统计与神经网络持续交汇；后来的方法并未取消此前的有效思想。

01

可计算的规则

1936：计算与边界
1956：AI研究纲领
符号、规则与搜索

02

概率与数据

不确定性进入模型
从样本估计参数
泛化成为中心问题

03

可学习的表示

多层网络与反传
2012：深度视觉突破
中间特征参与学习

04

可复用的系统

2017：Transformer
预训练与后训练
工具和长程任务

共同问题一直存在：怎样表示对象、利用经验，并在有限计算下作出有效判断？

符号与搜索：先定义合法空间，再寻找解

证明、棋类和早期专家系统的优势，来自明确的对象、规则与评价。



课程连接：问题形式化、搜索、引理检索、强化学习中的状态与动作。

贝叶斯更新：把含噪证据转成可比较的判断

量子测量、参数估计与实验选择都需要处理“信息不全时怎样更新”。

概率更新

$$p(h|D) = p(D|h) p(h) / p(D)$$

h : 假设或参数

D : 观测数据

竖线 “|” 表示 “在.....条件下”

1

先验

$p(h)$: 看到本批数据前
对假设 h 的判断

2

似然

$p(D|h)$: 假设 h 成立时
观测 D 出现的可能性

3

后验

$p(h|D)$: 看到 D 后
对 h 更新后的判断

4

归一化

$p(D)$: 所有候选共同解释数据的总概率

课程连接：概率输出、参数估计、不确定性；似然与后验不能混同。

反向传播让深层表示可以共同学习

把链式法则组织成高效计算；优化器随后使用梯度更新参数。



表达能力、可训练性、泛化能力是三个问题；损失下降只直接回答其中一部分。

深度学习突破来自数据、结构与计算的配合

AlexNet与后续视觉网络说明：算法必须在可训练、可比较的条件下兑现优势。



课程连接：卷积、参数共享、残差、初始化与泛化；结构假设必须适合数据。

AlphaGo到MuZero：学习与搜索相互增强

模型负责缩小搜索范围，搜索结果又为模型提供新的训练信号。

2016

AlphaGo

人类棋谱与自我对弈
策略建议走哪一步
价值估计局面好坏

2017-18

Zero系列

减少对棋谱的依赖
同一框架用于多类棋
仍给定规则与奖励

2020

MuZero

学习规划所需状态
预测奖励、价值
与任务相关的转移

课程接口

强化学习

状态、动作与奖励
价值估计与树搜索
模拟误差影响决策

成立条件：规则明确、试错便宜、反馈可靠；真实实验往往不具备全部条件。

Transformer与预训练，让能力成为可复用底座

2017年以来的关键变化：先学习通用表示，再用少量任务信息完成适配。



历史主线在此汇合：规则给约束，网络学表示，搜索与外部反馈改进结果。

先分清四个层次：学习方法、网络结构、底座与系统

人工智能是研究与工程目标；下列名称描述实现这一目标的不同层面。

方法

机器学习

从样本或反馈中学习
改进预测和决策
包括多种模型家族

结构

深度学习

使用多层可训练网络
中间表示随任务学习
并非所有AI都是深网

底座

基础模型

广泛训练后适配任务
处理一种或多种模态
不等于通用科学理论

系统

智能体

模型、工具与状态
按反馈选择后续动作
需要停止和检查条件

识别一个系统时，分别问：学什么、用什么结构、怎样调用、如何验证。

学习的最小问题：用数据选择一个预测函数

线性回归保留了后续复杂模型都要面对的输入、参数、目标与误差。

模型与误差

$$\hat{y} = wx + b$$
$$\text{单点损失} = (\hat{y} - y)^2 / 2$$

训练：让平均损失下降

测试：检查新样本上的误差

- 1 输入与目标**
x: 输入特征; y: 观测目标
 $\hat{y}$: 模型预测
- 2 模型参数**
w控制斜率, b控制偏移
训练时调整w和b
- 3 损失函数**
平方损失度量预测误差
平均多个样本后训练
- 4 泛化检验**
验证集用于选择设置
测试集用于最终评估

教学例： $x=2, y=4, w=1, b=0$; 预测 $\hat{y}=2$, 单点损失=2。

训练修改参数，推理使用参数完成当前任务

上下文适应、检索补充与重新训练，是三种不同的信息进入方式。

训练

把经验写入参数

样本 → 预测 → 损失 → 梯度
优化器更新模型参数
验证集监控过拟合

产出一个模型版本

推理

计算当前输入的输出

接收新的输入与上下文
可以采样、搜索、调用工具
通常不修改模型权重

完成一次预测或行动

≠

推理时增加计算可以改进搜索；缺失事实仍需新数据或外部证据。

表示决定模型实际看见哪些信息

编码不只是把对象变成数字，还要保留与任务有关的结构和单位。

文本

Token与嵌入

Token是计算单元
可为字、子词或符号
嵌入将其映射为向量

量子 / 工程

测量时间序列

保留顺序与采样间隔
区分状态变化与噪声
历史补充当前观测

自然科学

图与几何对象

原子是节点，关系是边
保留邻接与空间位置
旋转和编号不改含义

数学

公式与证明结构

保留变量、前提与依赖
向量相似帮助检索
相似不等于逻辑可用

课程连接：特征工程、向量内积、序列网络、图网络与位置表示。

注意力：根据当前查询，动态汇总相关信息

先算匹配分数，再归一化，最后对内容向量做加权汇总。

缩放点积注意力

$$\begin{aligned} S &= QK^T / \sqrt{d} \\ A &= \text{softmax}(S) \\ Z &= AV \end{aligned}$$

d: 查询与键的维度

T: 矩阵转置

softmax: 按行归一化

- 1** **Q、K、V** 查询Q、键K用于匹配值V提供被汇总的内容
- 2** **打分S** QK^T 逐对计算点积除以 $\sqrt{d}$ 控制数值尺度
- 3** **权重A** softmax逐行处理S得到非负且和为1的权重
- 4** **输出Z** $Z=AV$: 每个查询获得一个加权后的内容向量

手算：权重(0.75, 0.25)，内容(2, 6)，输出=3；注意力权重不是因果证据。

Transformer的能力来自一组协作的计算模块

以下是功能分解；具体模型的层顺序、归一化位置与结构可能不同。

01 输入与位置

将对象编码为向量，补充顺序或空间关系

02 自注意力

跨位置聚合信息；多头学习不同的匹配方式

03 前馈网络

在每个位置上做非线性变换，重组特征

04 残差与归一化

保留直通路径，控制中间数值与梯度尺度

05 输出头

把隐藏表示转为类别、数值或Token分布

结构与成本

标准全注意力
形成 $n \times n$ 关联

长序列需要
更高效的计算

课程连接：矩阵运算、非线性激活、反向传播、初始化、残差与归一化。

自监督学习：训练目标可以由数据自身产生

预测后续、遮盖重建和去噪学习提供不同信号；模型结构与训练目标应分开看。

预测目标

$$\text{单位置损失} = -\log p$$

p: 真实后续Token的预测概率

p=0.8 → 损失约0.223

p=0.2 → 损失约1.609

1

自回归

根据前文预测下一个Token
真实后续提供标签

2

遮盖重建

隐藏部分输入
利用剩余上下文恢复缺失内容

3

扩散去噪

训练时学习去噪
生成时逐步构造样本

4

迁移与局限

可学习通用表示
目标低误差不等于事实正确

课程连接：交叉熵、自监督、预训练与微调；材料和分子生成将再次使用去噪思想。

预训练、后训练与推理时计算解决不同瓶颈

不要把一次任务中的搜索，误认为模型又接受了大规模训练。



奖励和偏好是目标的代理：奖励变高，仍需检查真实任务是否完成。

扩大能力，同时降低每次有效计算的成本

规模、架构与推理效率共同演进；参数总量不足以解释模型表现。

规模

数据与计算配比

固定训练预算
匹配参数量与样本量
规模规律来自经验

稀疏

混合专家 MoE

路由选择部分子网络
每次激活部分参数
总参数 $\neq$ 单次计算量

序列

状态空间模型

递推状态汇总历史
降低长序列处理成本
信息压缩也有代价

部署

蒸馏与量化

蒸馏：小模型学教师
量化：减少数值位宽
必须重新评估误差

课程连接：计算复杂度、循环状态、参数共享与误差分析；效率也是算法问题。

外部增强：检索补证据，工具提供可执行能力

模型负责组织问题与解释结果；来源、执行和验证各自承担独立任务。

检索

RAG：把相关材料送入上下文

检索增强生成：先找，再生成
关键词或向量用于召回候选
保留来源并检查是否支持结论

检索命中不等于证据成立

工具

程序、数据库、模拟器与仪器

模型提出函数名与参数
外部程序执行并返回结果
根据真实反馈继续或修正

生成调用不等于执行成功

+

课程连接：向量检索、函数接口、误差核验；引理前提和实验单位必须逐项检查。

智能体把一次预测接成可反馈的任务过程

模型、工具、任务状态与验证器共同决定多步任务的可靠性。



多智能体可分工与并行；共享盲点不会因“多讨论几轮”自动消失。

多模态进入物理行动，闭环条件随之改变

语言、感知与控制需要在不同时间尺度上协作。



课程连接：序列表示、注意力、状态转移与强化学习；语言规划不替代高速控制。

能力评估必须同时改变任务与验证条件

模型在一个测试上表现好，不能直接推出跨分布、跨环境和长程任务可靠。



四方向共用的判断：新数据是否独立？对比是否公平？失效能否被发现？

自然语言接口，把非结构化信息接入可执行流程

技术增量在于任务结构化与工具执行；是否完成仍由返回结果判断。



例：实验记录 → 参数表 → 拟合脚本 → 残差检查；每一步都可独立评价。

模拟加速与候选生成，改变设计空间的探索方式

可以减少昂贵试算并扩大候选范围，但误差与约束必须沿流程传递。

01

代理模型

近似昂贵求解器
快速预测性能或演化
检查新工况误差

02

生成设计

由目标性质提出候选
分子、晶体、程序等
生成后仍需筛选验证

03

决策优化

比较收益、风险、成本
选择下次计算或实验
兼顾探索与利用

04

现实反馈

实测更新模型与候选
记录失败样本和偏差
识别仿真遗漏的机制

课程连接：回归代理、神经网络、图表示和强化学习；加速比必须连同误差报告。

反馈成为持续改进的数据，也可能形成新的偏差

部署会改变后续获得的数据；再训练之前，必须保留独立评价条件。



关键转移：候选生成更便宜后，高质量数据、验证与问题定义更加关键。

职业变化首先发生在任务组合与验证方式上

对本科生，更有用的判断是：哪些环节可以委派，哪些能力必须自己建立。



学习目标：从“交出一个答案”进步到“定义任务、实现算法、检验结果”。

三年级学生应积累可复核的能力证据

让AI承担重复劳动，同时让自己的数学、专业与计算能力留下清晰证据。

01

把问题写清

写清输入、输出、约束
辨认无法观测的条件
选择有意义的基线

02

把计算做实

复算损失与参数更新
运行并修改代码
核对维度、单位、边界

03

把错误找出

比较训练与测试表现
设计新条件下的检验
解释一个失败案例

04

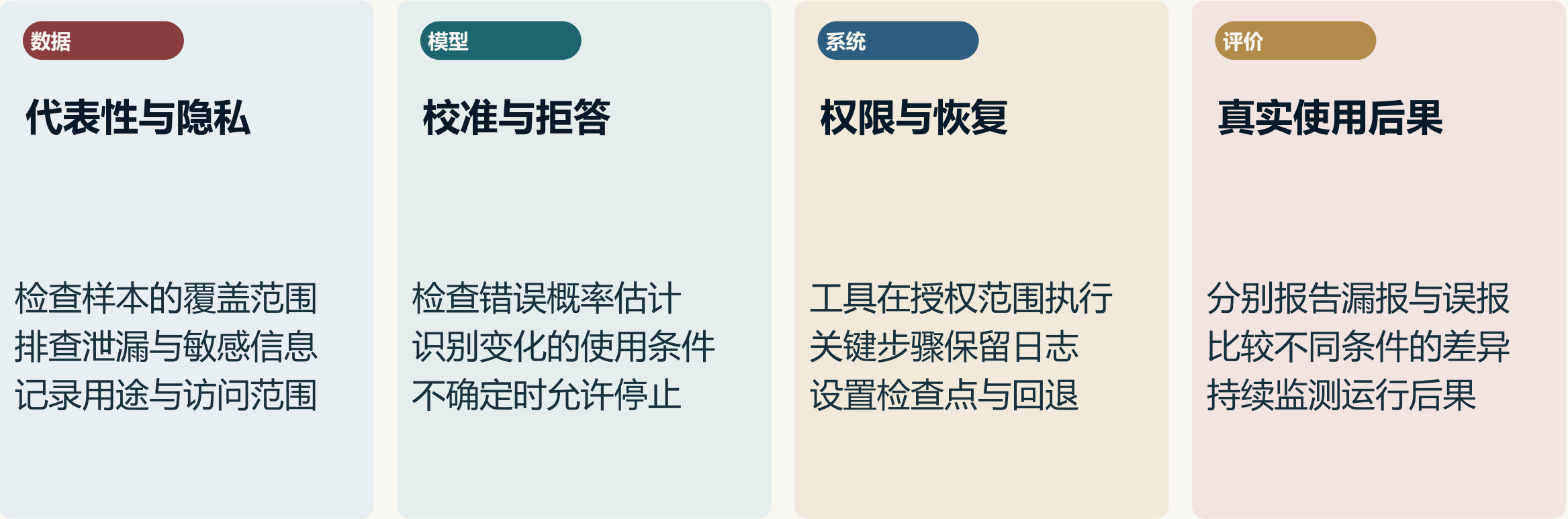
把成果说明

提供数据与版本来源
报告误差、成本、限制
现场解释为何有效

建议作品：一个小数据集 + 一个简单基线 + 一次方法改进 + 一份失败分析。

AI进入重要系统，可靠性必须成为设计变量

技术指标与使用后果相连：数据偏差、错误传播和责任需要可操作的处理机制。



社会问题可以落到技术接口：数据如何划分、阈值如何设定、失败由谁发现。

智能能力依赖物理资源与公共知识基础

算力、数据、软件与设施决定哪些方法能够训练、复现和长期使用。

计算

芯片与互联

训练：吞吐与通信
推理：延迟与显存
能耗属于实际成本

数据

测量与标准

测量需要校准与语义
单位、协议可追溯
开放数据降低门槛

软件

工具与可复现

记录软件库与环境
保存参数、依赖、种子
比较同预算的基线

设施

现实验证入口

实验装置与工程现场
提供模型之外的反馈
跨团队合作连接资源

对本课程：优先以小数据、小模型和可复现任务掌握原理，再理解前沿规模。

科学智能的任务，是把候选结果接回专业证据

同样使用神经网络，预测、生成、控制和机制发现所需的验证并不相同。



以下每个案例都回答：做哪一步？用什么算法？如何验证？与后续课程怎样连接？

AlphaFold 3：从分子组成预测复合体结构

Nature 2024；将蛋白质、核酸、小分子等纳入统一结构预测框架。

结构预测 | 2024

组成与序列
↓
三维复合体候选

输出是结构假设
独立实验与功能测定
提供不同层面的检验

1	任务	输入分子组成与相关信息 输出原子级结构候选
2	机制	学习分子间表示 使用扩散模块生成坐标
3	证据	与实验结构比较 置信度用于提示不可靠区域
4	课程接口	神经网络、注意力、结构表示 扩散属前沿延伸

结构预测帮助提出结合模式与实验优先级；结构本身不等于亲和力、动力学或功能。

生命科学模型：相似的规模化方法，不同的学习任务

区分序列预测、调控效应预测与功能设计，才能判断模型实际贡献。

2026

AlphaGenome

输入长DNA序列
预测表达、剪接等信号
比较变异前后的预测
课程：卷积、注意力
证据：任务数据与实验

2026

Evo 2

基因组序列建模
学习跨序列统计结构
用于评分与候选生成
课程：序列、自监督
边界：序列似然 $\neq$ 功能

2025

ESM3

联合序列、结构、功能
生成蛋白候选
部分候选获实验支持
课程：表示、条件生成
边界：样例成功 $\neq$ 通用

自然科学学生的准备：先明确一个实验标签、一个独立划分和一种功能验证。

MatterGen：在性质条件下生成晶体候选

Nature 2025；把材料设计从已有库筛选扩展到条件生成与后续验证。

材料设计 | 2025

目标条件

→ 晶体候选

→ 计算与实验

可直接起步：

先做材料性质回归

再比较候选筛选效率

1

对象

原子类型、位置与晶胞共同定义周期晶体

2

生成

条件扩散根据组成或性质要求构造候选

3

筛选

计算稳定性和目标性质
再选择实验对象

4

课程接口

图与几何表示、性质回归
生成模型为延伸

计算稳定、可合成、性能达标和可制造，是四个不同的判断。

自驱实验室：学习怎样使用下一次实验预算

自动执行提高吞吐；更有价值的目标是让每次实验改进判断。



课程连接：回归与概率基础；主动学习、贝叶斯优化作为应用延伸。

天气与地球系统：空间结构、概率与物理约束并行

不同路线分别解决快速预测、不确定性表达、物理一致性与任务迁移。

2023 GraphCast 图网络传递空间信息 学习后续天气状态 课程：图网络、回归 检验长时误差累积	2024 GenCast 生成多条可能轨迹 集合表达不确定性 联系：概率与生成 检验极端事件校准	2024 NeuralGCM 物理核心 + 学习模块 结合数值与数据方法 课程：反传与约束 检验长期稳定性	2025 Aurora 地球系统基础模型 适配多类预测任务 课程：预训练、微调 留出新区域与任务
---	---	--	---

第二讲将用GraphCast展开图网络入口；“预测更准”与“发现机制”分开评价。

聚变控制：预测只有进入动作反馈才形成控制能力

DIII-D研究 (Nature 2024) 展示基于学习的撕裂不稳定性规避。

闭环控制 | 2024

诊断信号
→ 风险预测
→ 动作与反馈

预测问：会发生什么？
控制问：怎样行动
才能改变后续结果？

- 1

观测

诊断信号估计装置状态
噪声和缺失影响判断
- 2

预测

估计未来失稳风险
为动作选择提供依据
- 3

策略

依据奖励和约束调整控制动作
并读取反馈
- 4

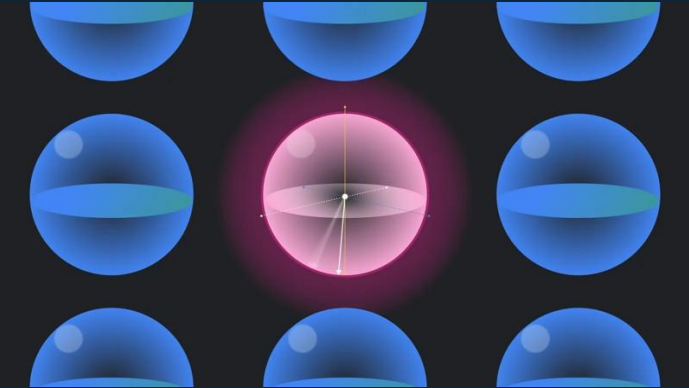
课程接口

序列模型、状态与动作、长期回报和强化学习

关键检验：动作延迟、约束满足、跨工况表现；控制成功不等于发现新物理。

AlphaQubit: 从测量历史推断逻辑错误

Nature 2024; 循环Transformer结合模拟预训练与实验数据微调。



AlphaQubit

经典模型处理含噪记录
量子装置提供独立反馈
精度与实时性共同评价

- 1

输入

稳定子测量历史提供纠错综合征及相关读出
- 2

学习

循环状态保留历史
注意力利用关联信息
- 3

输出

预测逻辑错误
同时评价误差率与解码耗时
- 4

课程接口

逻辑回归基线、序列网络、注意力与微调

这是经典AI帮助量子纠错；第二讲从简化解码任务展开，不要求复现完整系统。

数学与算法前沿：搜索能力必须配合合适的验证器

形式证明、自然语言论证和程序优化采用不同的证据标准。

形式证明

AlphaProof

搜索候选证明步骤
形式系统检查合法性
联系：搜索与奖励
先核对命题形式化

研究辅助

Aletheia | 2026

生成、核查、修改论证
自然语言验证仍会错
联系：推理时计算
需要数学专家审阅

程序搜索

AlphaEvolve

生成程序并自动评测
保留有效候选再迭代
联系：目标与搜索
测试覆盖范围有限

学生入口

小而强的验证

引理检索与反例搜索
比较关键词与向量法
用精确计算核验候选
报告前提和适用范围

第二讲分别展开引理检索、证明搜索、反例发现和数值近似。

符号规律发现：搜索方程之前，先审查变量与证据

并行符号枚举（NCS 2026）提高表达式搜索效率；它依赖给定变量和语法。

显式规律搜索

变量与语法
→ 候选表达式
→ 跨条件检验

正则化：限制模型复杂度
辨识：区分竞争的解释
闭合：状态足以描述演化

- 1

变量

数据里有哪些可观测量？是否遗漏关键状态？
- 2

表达式

允许哪些运算、组合和复杂度？检查量纲
- 3

辨识

不同公式可能拟合同一批数据
需要新条件区分
- 4

课程接口

回归、表示学习与正则化
符号发现为前沿延伸

公式简短、拟合误差小与机制成立是不同结论；跨条件预测和干预更有辨别力。

2026科研智能体：研究流程自动化正在接受实证检验

系统名称中的“科学家”不是证据；看它实际控制了哪一段研究流程。

01	02	03	04
AI co-scientist	Robin	Biomni	AI Scientist
生成、比较与改进假设 部分案例获实验支持 联系：搜索与反馈 边界：目标与验证	文献、分析与实验协同 人类参与真实实验 联系：工具与反馈 边界：并非无人研究	规划调用生物医学工具 完成数据分析任务 联系：任务分解、程序 边界：工具成功≠机制	选题与代码、实验写作 自动流程接受评测 联系：搜索、独立评价 边界：原创性与严谨性

可做的准备：先实现一个带来源、测试和错误记录的单工具研究助手。

科学智能的下一步，需要突破五类具体瓶颈

这些问题把算法研究与领域研究连接起来，也限定了当前成果的解释范围。



本科阶段的研究起点：选中一个瓶颈，在一个清楚的小任务上给出可复核改进。

产业地图要按掌握的能力与交付结果来读

机构案例用于辨认路径；融资和产品发布不能替代科学或工程验证。

01

通用与科学模型

DeepMind等：模型与评测
学生入口：复现、数据与误差分析

02

药物与分子研发

Isomorphic等：候选与研发管线
学生入口：性质预测与结构表示

03

自动实验平台

Lila、Periodic等：实验反馈
学生入口：数据质量与实验选择

04

开放科研工具

FutureHouse等：研究工具链
学生入口：检索、测试与工具接口

05

计算与研发平台

Microsoft等：算力、软件与流程
学生入口：仿真、效率与可复现

06

公共研究设施

高校与国家实验室：专业数据
学生入口：真实任务和领域合作

商业价值最终体现为研发效率、可验证成果或实际产品；学生先进入一段可完成的任务。

国家布局把算力、科学数据与设施组织到共同任务中

以下比较资源组织方式；计划目标与已经实现的研究能力应分别看待。

US

美国 | Genesis等

连接国家实验室、计算与科研数据
关注可计算挑战和设施接口

CN

中国 | 人工智能 +

科学研究、数据与重大设施协同
关注真实场景和学科合作

EU

欧盟 | AI in Science

连接研究人才、算力与数据资源
关注共享能力与可信使用

UK

英国 | 科学AI战略

围绕重点学科和研究任务部署
关注可评价的科学增量

JP

日本 | RIKEN

以研究机构、超算和模型协同
关注模拟与领域模型

你们

本科生的实际准备

加入一个有数据与导师的小问题
用专业判断检验算法贡献

选择研究机会时，先看问题、数据、指导与验证条件，再看平台名称和规模。

一个学期，形成一项能解释、能复现的小成果

以下是可调整的建议路径；围绕同一个专业问题逐步增加能力。



完成标准 **有数据、有基线、有独立测试** **有解释、有失败分析、有复现记录**

建议按专业基础与课程进度调整；每次增加一种能力，同时保留可归因的比较。

选择“一条专业主线 + 一个算法接口”，用完整证据积累研究能力。

四类专业，用不同任务进入共同算法基础

与第二讲的四方向一致：量子测量与控制、数学搜索与验证、实验预测、工程运行。

01

量子

入口：简化纠错
算法：分类、序列
联系：历史与注意力
检验：新噪声、延迟
先分清测量与标签

02

数学

入口：引理与反例
算法：向量与搜索
检验：前提、精确计算
先区分线索与证明

03

自然科学

入口：分子材料性质
算法：回归、图网络
检验：新结构、实验
先核对单位与标签

04

工程

入口：诊断与优化
算法：分类、序列
联系：决策与约束
检验：新设备、成本
先定义使用条件

四个方向都从同一件事开始：把一个真实问题，变成可学习、可比较、可验证的任务。

后续算法课，将拆开前沿系统中的这些关键环节

与第二讲算法导读对应；扩散、贝叶斯优化和符号发现作为前沿联系与延伸。

01 预测与优化

线性 / 逻辑回归、损失、梯度下降与泛化

02 表示与训练

网络、反传、初始化与训练稳定性

03 时间与关系

RNN、LSTM、GRU；图表示与图卷积

04 关联与预训练

注意力与Transformer
自监督、预训练与微调

05 行动与长期收益

状态、动作、奖励；MDP、Q学习与DQN

对应前沿

AlphaQubit
历史与关联
GraphCast
空间关系
聚变控制
长期决策

每学一种方法，都追问：它改善了哪个环节？需要什么数据？新增了什么误差或代价？

带着一张任务卡，进入第二讲的四方向应用

选择一个专业入口，写清输入、输出、基线与验证；随后从线性回归开始计算。

01

对象

一条样本是什么？
输入与目标是什么？

02

方法

最简单的基线是什么？
AI准备改善哪一步？

03

证据

用什么新条件检验？
怎样判定方法失败？

任务卡：一个具体输出 + 一个比较基线 + 一种失败判据。

下一讲：定义问题 → 准备数据 → 建立基线 → 训练改进 → 独立验证。