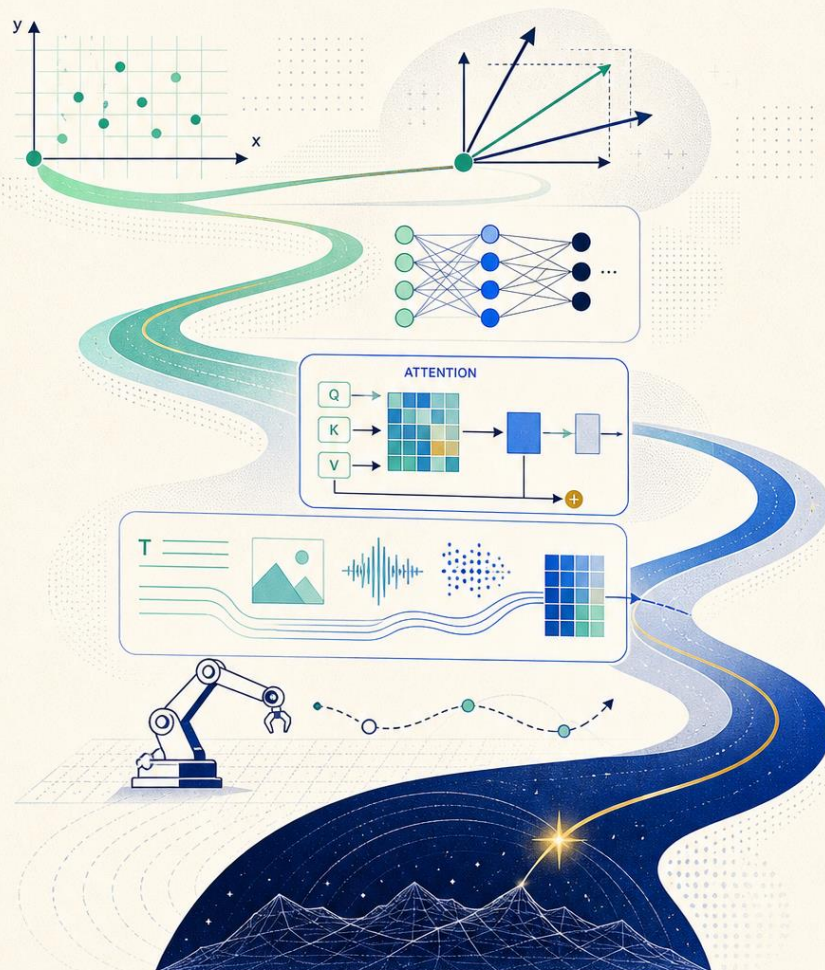


从零开始学AI

普通人与高中生的24个月互动教材

2026.08 Beta



NEWVAR

第三卷：主要 AI 分支

版本、边界与使用方法

结论先行：这是一套面向普通人与高中生的系统教材，不是速成承诺。当前为 **2026.08 Beta**；只有技术评审、事实核查和领域专家签字全部完成后，才能进入 stable。

项目	内容
版本	2026.08 Beta
卷册	第三卷：主要 AI 分支
本卷章节	24
全书结构	4 卷 · 24 单元 · 96 章
实践资产	96 个互动实验 · 24 个项目 · 288 道练习
正文规模	约 689,651 个汉字
核实日期	2026-08-06
版权	Copyright © 2026 NEWVAR LAB. All rights reserved.

能力终点

本书以独立开发、部署、论文阅读、实验复现、失败分析和研究问题提出为终点能力；不承诺仅靠一本书自动成为世界顶尖研究者。

全面覆盖的可审计边界

“全面”指对主要 AI 知识域、能力框架、工程链路和研究方法进行可审计覆盖，不等于收录互联网上每一页资料。

每章学习契约

- 先看结论、价值和完成后能做什么。
- 完成先修检查，用生活类比获得方向，再主动找出类比失效处。
- 一次只改变一个核心变量；网页提供键盘操作和静态替代说明。
- 按直觉、数学、最小实现、PyTorch、实验、失败、迁移的顺序推进。
- 工程线与研究线至少选择一条；三级练习先独立完成，再看答案。
- 所有结果必须标成实际测量、教学模拟或文献引用；不能混写。
- 遇到高风险决策、隐私数据或证据不足时停止自动化并交给给人。

隐私与材料规则

全书案例只使用虚构或公开数据。不要在练习、截图、Notebook 或网站笔记中输入姓名、账号、联系方式、密钥、医疗记录、成绩等个人信息。网页学习记录仅保存在当前设备，可匿名导入导出；不建账号、不做行为追踪。

目录

目录由 Word 字段生成。打开文件后若页码尚未刷新，请按 Ctrl+A，再按 F9。

版本、边界与使用方法..... 2

 能力终点..... 2

 全面覆盖的可审计边界..... 3

 每章学习契约..... 3

 隐私与材料规则..... 3

目录..... 4

本卷 24 章路线图..... 35

 月 13 · 计算机视觉..... 35

 月 14 · 自然语言处理..... 35

 月 15 · 语音与音频..... 35

 月 16 · 生成模型、扩散与流模型..... 36

 月 17 · 强化学习与控制..... 36

 月 18 · 机器人与具身智能..... 36

第 49 章 像素、颜色与卷积..... 38

 1. 为什么重要，现在能做什么..... 38

 2. 先修检查与生活类比..... 39

 3. 互动实验：只改变一个变量..... 39

 4. 直觉到数学..... 40

 5. 最小实现..... 40

6. 五轮系统化理解	41
1. 问题边界	41
3. 机制与因果链	42
7. 评估与不确定性	43
9. 工程与复现	44
11. 迁移与研究	45
7. PyTorch 实现路线	47
8. 实验设计与结果记录	47
9. 常见失败与排查顺序	47
10. 迁移任务	48
11. 三级练习	48
12. 本章能力检查	49
13. 来源与核实	49
第 50 章 CNN、残差网络与迁移学习	50
1. 为什么重要，现在能做什么	50
2. 先修检查与生活类比	51
3. 互动实验：只改变一个变量	51
4. 直觉到数学	52
5. 最小实现	52
6. 五轮系统化理解	53
1. 问题边界	53

3. 机制与因果链.....	54
7. 评估与不确定性	55
9. 工程与复现	56
11. 迁移与研究	57
7. PyTorch 实现路线	59
8. 实验设计与结果记录	59
9. 常见失败与排查顺序	59
10. 迁移任务.....	60
11. 三级练习.....	60
12. 本章能力检查.....	61
13. 来源与核实	61
第 51 章 目标检测、分割与结构化输出.....	62
1. 为什么重要，现在能做什么.....	62
2. 先修检查与生活类比	63
3. 互动实验：只改变一个变量.....	63
4. 直觉到数学	64
5. 最小实现.....	64
6. 五轮系统化理解	65
1. 问题边界.....	65
3. 机制与因果链.....	66
7. 评估与不确定性	67

9. 工程与复现	68
11. 迁移与研究	69
7. PyTorch 实现路线	71
8. 实验设计与结果记录	71
9. 常见失败与排查顺序	71
10. 迁移任务	72
11. 三级练习	72
12. 本章能力检查	73
13. 来源与核实	73
第 52 章 视觉 Transformer、生成视觉与评估	74
1. 为什么重要，现在能做什么	74
2. 先修检查与生活类比	75
3. 互动实验：只改变一个变量	75
4. 直觉到数学	76
5. 最小实现	76
6. 五轮系统化理解	77
1. 问题边界	77
3. 机制与因果链	78
7. 评估与不确定性	79
9. 工程与复现	80
11. 迁移与研究	81

7. PyTorch 实现路线	83
8. 实验设计与结果记录	83
9. 常见失败与排查顺序	83
10. 迁移任务	84
11. 三级练习	84
12. 本章能力检查	85
13. 来源与核实	85
月 13 阶段项目：制作一个公开图像数据的可解释识别器	86
交付物	86
验收方法	86
第 53 章 文本、Unicode、分词与词元	87
1. 为什么重要，现在能做什么	87
2. 先修检查与生活类比	88
3. 互动实验：只改变一个变量	88
4. 直觉到数学	89
5. 最小实现	89
6. 五轮系统化理解	90
1. 问题边界	90
3. 机制与因果链	91
7. 评估与不确定性	92
9. 工程与复现	93

11. 迁移与研究	94
7. PyTorch 实现路线	95
8. 实验设计与结果记录	96
9. 常见失败与排查顺序	96
10. 迁移任务	97
11. 三级练习	97
12. 本章能力检查	97
13. 来源与核实	98
第 54 章 词向量、RNN 与 LSTM	99
1. 为什么重要，现在能做什么	99
2. 先修检查与生活类比	100
3. 互动实验：只改变一个变量	100
4. 直觉到数学	101
5. 最小实现	101
6. 五轮系统化理解	102
1. 问题边界	102
3. 机制与因果链	103
7. 评估与不确定性	104
9. 工程与复现	105
11. 迁移与研究	106
7. PyTorch 实现路线	108

8. 实验设计与结果记录	108
9. 常见失败与排查顺序	108
10. 迁移任务	109
11. 三级练习	109
12. 本章能力检查	110
13. 来源与核实	110
第 55 章 注意力与 Transformer	111
1. 为什么重要，现在能做什么	111
2. 先修检查与生活类比	112
3. 互动实验：只改变一个变量	112
4. 直觉到数学	113
5. 最小实现	113
6. 五轮系统化理解	114
1. 问题边界	114
3. 机制与因果链	115
7. 评估与不确定性	116
9. 工程与复现	117
11. 迁移与研究	118
7. PyTorch 实现路线	119
8. 实验设计与结果记录	120
9. 常见失败与排查顺序	120

10. 迁移任务	121
11. 三级练习	121
12. 本章能力检查	121
13. 来源与核实	122
第 56 章 NLP 任务、检索、评估与责任	123
1. 为什么重要，现在能做什么	123
2. 先修检查与生活类比	124
3. 互动实验：只改变一个变量	124
4. 直觉到数学	125
5. 最小实现	125
6. 五轮系统化理解	126
1. 问题边界	126
3. 机制与因果链	127
7. 评估与不确定性	128
9. 工程与复现	129
11. 迁移与研究	131
7. PyTorch 实现路线	132
8. 实验设计与结果记录	132
9. 常见失败与排查顺序	133
10. 迁移任务	133
11. 三级练习	133

12. 本章能力检查	134
13. 来源与核实	134
月 14 阶段项目：做一个带检索证据的校园 FAQ 原型	136
交付物	136
验收方法	136
第 57 章 波形、采样与短时傅里叶变换	137
1. 为什么重要，现在能做什么	137
2. 先修检查与生活类比	138
3. 互动实验：只改变一个变量	138
4. 直觉到数学	139
5. 最小实现	139
6. 五轮系统化理解	140
1. 问题边界	140
3. 机制与因果链	141
7. 评估与不确定性	142
9. 工程与复现	143
11. 迁移与研究	145
7. PyTorch 实现路线	146
8. 实验设计与结果记录	146
9. 常见失败与排查顺序	147
10. 迁移任务	147

11. 三级练习	147
12. 本章能力检查	148
13. 来源与核实	148
第 58 章 自动语音识别：声音到文字	149
1. 为什么重要，现在能做什么	149
2. 先修检查与生活类比	150
3. 互动实验：只改变一个变量	150
4. 直觉到数学	151
5. 最小实现	151
6. 五轮系统化理解	152
1. 问题边界	152
3. 机制与因果链	153
7. 评估与不确定性	154
9. 工程与复现	155
11. 迁移与研究	156
7. PyTorch 实现路线	157
8. 实验设计与结果记录	158
9. 常见失败与排查顺序	158
10. 迁移任务	159
11. 三级练习	159
12. 本章能力检查	159

13. 来源与核实	160
第 59 章 语音合成与声码器	161
1. 为什么重要，现在能做什么	161
2. 先修检查与生活类比	162
3. 互动实验：只改变一个变量	162
4. 直觉到数学	163
5. 最小实现	163
6. 五轮系统化理解	164
1. 问题边界	164
3. 机制与因果链	165
7. 评估与不确定性	166
9. 工程与复现	167
11. 迁移与研究	168
7. PyTorch 实现路线	170
8. 实验设计与结果记录	170
9. 常见失败与排查顺序	170
10. 迁移任务	171
11. 三级练习	171
12. 本章能力检查	172
13. 来源与核实	172
第 60 章 音频理解、音乐与说话人隐私	173

1. 为什么重要，现在能做什么	173
2. 先修检查与生活类比	174
3. 互动实验：只改变一个变量	174
4. 直觉到数学	175
5. 最小实现	175
6. 五轮系统化理解	176
1. 问题边界	176
3. 机制与因果链	177
7. 评估与不确定性	178
9. 工程与复现	179
11. 迁移与研究	180
7. PyTorch 实现路线	182
8. 实验设计与结果记录	182
9. 常见失败与排查顺序	182
10. 迁移任务	183
11. 三级练习	183
12. 本章能力检查	184
13. 来源与核实	184
月 15 阶段项目：制作一个不上传声音的本地音频分类实验	185
交付物	185
验收方法	185

第 61 章 生成建模与变分自编码器.....	186
1. 为什么重要，现在能做什么.....	186
2. 先修检查与生活类比	187
3. 互动实验：只改变一个变量.....	187
4. 直觉到数学	188
5. 最小实现.....	188
6. 五轮系统化理解	189
1. 问题边界.....	189
3. 机制与因果链.....	190
7. 评估与不确定性	191
9. 工程与复现	192
11. 迁移与研究	193
7. PyTorch 实现路线	195
8. 实验设计与结果记录	195
9. 常见失败与排查顺序	195
10. 迁移任务.....	196
11. 三级练习.....	196
12. 本章能力检查.....	197
13. 来源与核实	197
第 62 章 生成对抗网络	198
1. 为什么重要，现在能做什么.....	198

2. 先修检查与生活类比	199
3. 互动实验：只改变一个变量.....	199
4. 直觉到数学	200
5. 最小实现.....	200
6. 五轮系统化理解	201
1. 问题边界.....	201
3. 机制与因果链.....	202
7. 评估与不确定性	203
9. 工程与复现	204
11. 迁移与研究	205
7. PyTorch 实现路线	207
8. 实验设计与结果记录	207
9. 常见失败与排查顺序	207
10. 迁移任务.....	208
11. 三级练习.....	208
12. 本章能力检查.....	209
13. 来源与核实	209
第 63 章 扩散模型与分数匹配.....	210
1. 为什么重要，现在能做什么.....	210
2. 先修检查与生活类比	211
3. 互动实验：只改变一个变量.....	211

4. 直觉到数学	212
5. 最小实现.....	212
6. 五轮系统化理解	213
1. 问题边界.....	213
3. 机制与因果链.....	214
7. 评估与不确定性	215
9. 工程与复现	216
11. 迁移与研究	217
7. PyTorch 实现路线	218
8. 实验设计与结果记录	219
9. 常见失败与排查顺序	219
10. 迁移任务.....	220
11. 三级练习.....	220
12. 本章能力检查.....	220
13. 来源与核实	221
第 64 章 流模型、能量模型与生成评估.....	222
1. 为什么重要，现在能做什么.....	222
2. 先修检查与生活类比	223
3. 互动实验：只改变一个变量.....	223
4. 直觉到数学	224
5. 最小实现.....	224

6. 五轮系统化理解	225
1. 问题边界	225
3. 机制与因果链	226
7. 评估与不确定性	227
9. 工程与复现	228
11. 迁移与研究	229
7. PyTorch 实现路线	231
8. 实验设计与结果记录	231
9. 常见失败与排查顺序	231
10. 迁移任务	232
11. 三级练习	232
12. 本章能力检查	233
13. 来源与核实	233
月 16 阶段项目：生成并审计一组教学模拟图案	234
交付物	234
验收方法	234
第 65 章 MDP、回报与贝尔曼方程	235
1. 为什么重要，现在能做什么	235
2. 先修检查与生活类比	236
3. 互动实验：只改变一个变量	236
4. 直觉到数学	237

5. 最小实现.....	237
6. 五轮系统化理解	238
1. 问题边界.....	238
3. 机制与因果链.....	239
7. 评估与不确定性	240
9. 工程与复现	241
11. 迁移与研究	243
7. PyTorch 实现路线	244
8. 实验设计与结果记录	244
9. 常见失败与排查顺序	245
10. 迁移任务.....	245
11. 三级练习.....	245
12. 本章能力检查.....	246
13. 来源与核实	246
第 66 章 价值学习、Q-learning 与 DQN.....	248
1. 为什么重要，现在能做什么.....	248
2. 先修检查与生活类比	249
3. 互动实验：只改变一个变量.....	249
4. 直觉到数学	250
5. 最小实现.....	250
6. 五轮系统化理解	251

1. 问题边界	251
3. 机制与因果链	252
7. 评估与不确定性	253
9. 工程与复现	254
11. 迁移与研究	255
7. PyTorch 实现路线	257
8. 实验设计与结果记录	257
9. 常见失败与排查顺序	257
10. 迁移任务	258
11. 三级练习	258
12. 本章能力检查	259
13. 来源与核实	259
第 67 章 策略梯度、Actor-Critic 与 PPO	260
1. 为什么重要，现在能做什么	260
2. 先修检查与生活类比	261
3. 互动实验：只改变一个变量	261
4. 直觉到数学	262
5. 最小实现	262
6. 五轮系统化理解	263
1. 问题边界	263
3. 机制与因果链	264

7. 评估与不确定性	265
9. 工程与复现	266
11. 迁移与研究	267
7. PyTorch 实现路线	269
8. 实验设计与结果记录	269
9. 常见失败与排查顺序	269
10. 迁移任务	270
11. 三级练习	270
12. 本章能力检查	271
13. 来源与核实	271
第 68 章 模型式、离线、多智能体与安全 RL	272
1. 为什么重要，现在能做什么	272
2. 先修检查与生活类比	273
3. 互动实验：只改变一个变量	273
4. 直觉到数学	274
5. 最小实现	274
6. 五轮系统化理解	275
1. 问题边界	275
3. 机制与因果链	276
7. 评估与不确定性	277
9. 工程与复现	278

11. 迁移与研究	280
7. PyTorch 实现路线	281
8. 实验设计与结果记录	281
9. 常见失败与排查顺序	282
10. 迁移任务	282
11. 三级练习	282
12. 本章能力检查	283
13. 来源与核实	283
月 17 阶段项目：训练一个可解释的网格世界智能体	285
交付物	285
验收方法	285
第 69 章 坐标、运动学与动力学	286
1. 为什么重要，现在能做什么	286
2. 先修检查与生活类比	287
3. 互动实验：只改变一个变量	287
4. 直觉到数学	288
5. 最小实现	288
6. 五轮系统化理解	289
1. 问题边界	289
3. 机制与因果链	290
7. 评估与不确定性	291

9. 工程与复现	292
11. 迁移与研究	293
7. PyTorch 实现路线	294
8. 实验设计与结果记录	295
9. 常见失败与排查顺序	295
10. 迁移任务	296
11. 三级练习	296
12. 本章能力检查	296
13. 来源与核实	297
第 70 章 传感、定位、地图与 SLAM	298
1. 为什么重要，现在能做什么	298
2. 先修检查与生活类比	299
3. 互动实验：只改变一个变量	299
4. 直觉到数学	300
5. 最小实现	300
6. 五轮系统化理解	301
1. 问题边界	301
3. 机制与因果链	302
7. 评估与不确定性	303
9. 工程与复现	304
11. 迁移与研究	305

7. PyTorch 实现路线	306
8. 实验设计与结果记录	307
9. 常见失败与排查顺序	307
10. 迁移任务	308
11. 三级练习	308
12. 本章能力检查	308
13. 来源与核实	309
第 71 章 运动规划与反馈控制	310
1. 为什么重要，现在能做什么	310
2. 先修检查与生活类比	311
3. 互动实验：只改变一个变量	311
4. 直觉到数学	312
5. 最小实现	312
6. 五轮系统化理解	313
1. 问题边界	313
3. 机制与因果链	314
7. 评估与不确定性	315
9. 工程与复现	316
11. 迁移与研究	317
7. PyTorch 实现路线	319
8. 实验设计与结果记录	319

9. 常见失败与排查顺序	319
10. 迁移任务	320
11. 三级练习	320
12. 本章能力检查	321
13. 来源与核实	321
第 72 章 机器人学习、仿真到现实与人身安全	322
1. 为什么重要，现在能做什么	322
2. 先修检查与生活类比	323
3. 互动实验：只改变一个变量	323
4. 直觉到数学	324
5. 最小实现	324
6. 五轮系统化理解	325
1. 问题边界	325
3. 机制与因果链	326
7. 评估与不确定性	327
9. 工程与复现	328
11. 迁移与研究	329
7. PyTorch 实现路线	331
8. 实验设计与结果记录	331
9. 常见失败与排查顺序	331
10. 迁移任务	332

11. 三级练习	332
12. 本章能力检查	333
13. 来源与核实	333
月 18 阶段项目：搭建一个二维机器人安全导航模拟器	334
交付物	334
验收方法	334
独立练习答案	335
第 49 章答案 · 像素、颜色与卷积	335
基础题参考	335
应用题参考	335
挑战题参考	335
自评量规	335
第 50 章答案 · CNN、残差网络与迁移学习	336
基础题参考	336
应用题参考	336
挑战题参考	336
自评量规	336
第 51 章答案 · 目标检测、分割与结构化输出	337
基础题参考	337
应用题参考	337
挑战题参考	337

自评量规.....	337
第 52 章答案 · 视觉 Transformer、生成视觉与评估.....	338
基础题参考	338
应用题参考	338
挑战题参考	338
自评量规.....	338
第 53 章答案 · 文本、Unicode、分词与词元.....	339
基础题参考	339
应用题参考	339
挑战题参考	339
自评量规.....	339
第 54 章答案 · 词向量、RNN 与 LSTM	340
基础题参考	340
应用题参考	340
挑战题参考	340
自评量规.....	340
第 55 章答案 · 注意力与 Transformer.....	341
基础题参考	341
应用题参考	341
挑战题参考	341
自评量规.....	341

第 56 章答案 · NLP 任务、检索、评估与责任	342
基础题参考	342
应用题参考	342
挑战题参考	342
自评量规	342
第 57 章答案 · 波形、采样与短时傅里叶变换	343
基础题参考	343
应用题参考	343
挑战题参考	343
自评量规	343
第 58 章答案 · 自动语音识别：声音到文字	344
基础题参考	344
应用题参考	344
挑战题参考	344
自评量规	344
第 59 章答案 · 语音合成与声码器	345
基础题参考	345
应用题参考	345
挑战题参考	345
自评量规	345
第 60 章答案 · 音频理解、音乐与说话人隐私	346

基础题参考	346
应用题参考	346
挑战题参考	346
自评量规.....	346
第 61 章答案 · 生成建模与变分自编码器	347
基础题参考	347
应用题参考	347
挑战题参考	347
自评量规.....	347
第 62 章答案 · 生成对抗网络.....	348
基础题参考	348
应用题参考	348
挑战题参考	348
自评量规.....	348
第 63 章答案 · 扩散模型与分数匹配	349
基础题参考	349
应用题参考	349
挑战题参考	349
自评量规.....	349
第 64 章答案 · 流模型、能量模型与生成评估	350
基础题参考	350

应用题参考	350
挑战题参考	350
自评量规.....	350
第 65 章答案 · MDP、回报与贝尔曼方程.....	351
基础题参考	351
应用题参考	351
挑战题参考	351
自评量规.....	351
第 66 章答案 · 价值学习、Q-learning 与 DQN	352
基础题参考	352
应用题参考	352
挑战题参考	352
自评量规.....	352
第 67 章答案 · 策略梯度、Actor-Critic 与 PPO	353
基础题参考	353
应用题参考	353
挑战题参考	353
自评量规.....	353
第 68 章答案 · 模型式、离线、多智能体与安全 RL.....	354
基础题参考	354
应用题参考	354

挑战题参考	354
自评量规.....	354
第 69 章答案 · 坐标、运动学与动力学.....	355
基础题参考	355
应用题参考	355
挑战题参考	355
自评量规.....	355
第 70 章答案 · 传感、定位、地图与 SLAM	356
基础题参考	356
应用题参考	356
挑战题参考	356
自评量规.....	356
第 71 章答案 · 运动规划与反馈控制	357
基础题参考	357
应用题参考	357
挑战题参考	357
自评量规.....	357
第 72 章答案 · 机器人学习、仿真到现实与人身安全.....	358
基础题参考	358
应用题参考	358
挑战题参考	358

自评量规.....	358
本卷来源台账.....	360
[S017] CS221: Artificial Intelligence	360
[S026] CS231n: Deep Learning for Computer Vision.....	360
[S027] Deep Residual Learning for Image Recognition	361
[S028] An Image is Worth 16x16 Words.....	361
[S029] CS224N: Natural Language Processing with Deep Learning	362
[S030] Attention Is All You Need	363
[S031] BERT: Pre-training of Deep Bidirectional Transformers.....	363
[S032] TorchAudio Documentation	364
[S033] Deep Speech	364
[S034] WaveNet.....	365
[S035] Auto-Encoding Variational Bayes	366
[S036] Generative Adversarial Nets	366
[S037] Denoising Diffusion Probabilistic Models.....	367
[S038] Score-Based Generative Modeling through Stochastic Differential Equations	367
[S039] Flow Matching for Generative Modeling.....	368
[S040] Reinforcement Learning: An Introduction.....	369
[S041] CS 285: Deep Reinforcement Learning	369
[S042] Human-level control through deep reinforcement learning.....	370
[S043] Proximal Policy Optimization Algorithms	370

[S044] ROS 2 Documentation	371
[S045] Probabilistic Robotics.....	371
[S055] Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks.....	372
[S071] Model Cards for Model Reporting.....	372
全书术语表	374
版权、版本与勘误.....	384

本卷 24 章路线图

月 13 · 计算机视觉

理解采样、通道、局部感受野、卷积核和等变性。

1. [第 49 章 像素、颜色与卷积 — 理解采样、通道、局部感受野、卷积核和等变性。](#)
2. [第 50 章 CNN、残差网络与迁移学习 — 理解层级特征、残差连接、预训练和领域差异。](#)
3. [第 51 章 目标检测、分割与结构化输出 — 区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。](#)
4. [第 52 章 视觉 Transformer、生成视觉与评估 — 理解图像分块、全局注意力、生成质量评估和数据偏见。](#)

月 14 · 自然语言处理

理解字符、字节、规范化、词、子词和词表外问题。

5. [第 53 章 文本、Unicode、分词与词元 — 理解字符、字节、规范化、词、子词和词表外问题。](#)
6. [第 54 章 词向量、RNN 与 LSTM — 理解分布式表示、序列状态、长程依赖和门控记忆。](#)
7. [第 55 章 注意力与 Transformer — 从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。](#)
8. [第 56 章 NLP 任务、检索、评估与责任 — 覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。](#)

月 15 · 语音与音频

理解采样率、混叠、频率、相位、窗口和时频图。

9. [第 57 章 波形、采样与短时傅里叶变换 — 理解采样率、混叠、频率、相位、窗口和时频图。](#)
10. [第 58 章 自动语音识别：声音到文字 — 理解声学表示、语言信息、CTC 或序列到序列和字错率。](#)
11. [第 59 章 语音合成与声码器 — 理解文本前端、声学模型、声码器、韵律和说话人控制的风险。](#)

12. [第 60 章 音频理解、音乐与说话人隐私 — 覆盖事件检测、音乐表示、说话人识别与匿名化边界。](#)

月 16 · 生成模型、扩散与流模型

区分显式、隐式生成，理解潜变量、重参数化和证据下界。

13. [第 61 章 生成建模与变分自编码器 — 区分显式、隐式生成，理解潜变量、重参数化和证据下界。](#)

14. [第 62 章 生成对抗网络 — 理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。](#)

15. [第 63 章 扩散模型与分数匹配 — 理解加噪、去噪、分数函数、采样步数和条件引导。](#)

16. [第 64 章 流模型、能量模型与生成评估 — 理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。](#)

月 17 · 强化学习与控制

理解状态、动作、转移、奖励、折扣和马尔可夫假设。

17. [第 65 章 MDP、回报与贝尔曼方程 — 理解状态、动作、转移、奖励、折扣和马尔可夫假设。](#)

18. [第 66 章 价值学习、Q-learning 与 DQN — 从时序差分更新到经验回放、目标网络和过估计问题。](#)

19. [第 67 章 策略梯度、Actor-Critic 与 PPO — 直接优化策略概率，用价值基线降方差，理解裁剪目标。](#)

20. [第 68 章 模型式、离线、多智能体与安全 RL — 理解环境模型、分布外动作、信用分配、约束和安全探索。](#)

月 18 · 机器人与具身智能

理解坐标系、位姿、关节、正逆运动学、速度与力。

21. [第 69 章 坐标、运动学与动力学 — 理解坐标系、位姿、关节、正逆运动学、速度与力。](#)

22. [第 70 章 传感、定位、地图与 SLAM — 融合带噪观测，在未知环境同时估计位姿与地图。](#)

23. [第 71 章 运动规划与反馈控制 — 区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。](#)

24. [第 72 章 机器人学习、仿真到现实与人身安全 — 理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。](#)

第 49 章 像素、颜色与卷积

Image representation and convolution

项目	内容
学习单元	月 13 · 计算机视觉
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：[第 48 章 PyTorch 工程：数据、检查点与推理](#)

结论先行：理解采样、通道、局部感受野、卷积核和等变性。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“像素、颜色与卷积”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解采样、通道、局部感受野、卷积核和等变性。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 `pytorch-engineering`。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。类比的值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 49-1 像素、颜色与卷积：单变量实验（教学模拟）

项目	内容
只改变量	卷积核尺寸，范围 1–11，步长 2
实验目标	只改变“卷积核尺寸”，观察结果、代价和风险如何一起变化，理解理解采样、通道、局部感受野、卷积核和等变性。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把卷积核尺寸分别设为 1、3 和 11，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“卷积核尺寸”，观察结果、代价和风险如何一起变化，理解理解采样、通道、局部感受野、卷积核和等变性。

静态替代说明：静态替代：把卷积核尺寸分别设为 1、3 和 11，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $y[i,j]=\sum_m\sum_n k[m,n]x[i-m,j-n]$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 49-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“像素、颜色与卷积”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解采样、通道、局部感受野、卷积核和等变性。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用不含个人信息的教学模拟天气记录建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成音频波形与环境声标签作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“卷积核尺寸”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失

败样例。对于 $y[i,j]=\sum_m\sum_n k[m,n]x[i-m,j-n]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在不含个人信息的教学模拟天气记录中，当卷积核尺寸变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“像素、颜色与卷积”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解采样、通道、局部感受野、卷积核和等变性。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园能源使用的匿名汇总数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园图书馆的公开借阅类别作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“卷积核尺寸”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、

边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $y[i,j]=\sum_m\sum_n k[m,n]x[i-m,j-n]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园能源使用的匿名汇总数据中，当卷积核尺寸变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“像素、颜色与卷积”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解采样、通道、局部感受野、卷积核和等变性。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园能源使用的匿名汇总数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低

可接受表现是什么？再把校园图书馆的公开借阅类别作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“卷积核尺寸”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $y[i,j]=\sum_m\sum_n k[m,n]x[i-m,j-n]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在校园能源使用的匿名汇总数据中，当卷积核尺寸变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“像素、颜色与卷积”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解采样、通道、局部感受野、卷积核和等变性。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用不含个人信息的教学模拟天气记录建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成音频波形与环境声标签作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“卷积核尺寸”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $y[i,j]=\sum_m\sum_n k[m,n]x[i-m,j-n]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在不含个人信息的教学模拟天气记录中，当卷积核尺寸变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“像素、颜色与卷积”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解采样、通道、局部感受野、卷积核和等变性。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论

和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园能源使用的匿名汇总数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园图书馆的公开借阅类别作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“卷积核尺寸”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $y[i,j]=\sum_m\sum_n k[m,n]x[i-m,j-n]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园能源使用的匿名汇总数据中，当卷积核尺寸变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“卷积核尺寸”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

25. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。

26. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。

27. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

28. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

29. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

30. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

31. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择不含个人信息的教学模拟天气记录作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择公开天文观测的缩小样例，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

32. **基础题：** 用自己的话解释“像素、颜色与卷积”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

33. **应用题：** 在合成的植物叶片特征中设计一个只改变“卷积核尺寸”的实验，列出基线、三档设置、指标和失败样例。

34. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/image-representation-convolution.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S026] Stanford University, 《CS231n: Deep Learning for Computer Vision》，[访问 cs231n.stanford.edu](https://cs231n.stanford.edu))
- [S027] Kaiming He et al., 《Deep Residual Learning for Image Recognition》，[访问 arxiv.org](https://arxiv.org))
- [S028] Alexey Dosovitskiy et al., 《An Image is Worth 16x16 Words》，[访问 arxiv.org](https://arxiv.org))
- [S071] Margaret Mitchell et al., 《Model Cards for Model Reporting》，[访问 arxiv.org](https://arxiv.org))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 50 章 CNN、残差网络与迁移学习

CNNs, ResNets and transfer

项目	内容
学习单元	月 13 · 计算机视觉
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：[第 49 章 像素、颜色与卷积](#)

结论先行： 理解层级特征、残差连接、预训练和领域差异。 **版本边界：** 本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“CNN、残差网络与迁移学习”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解层级特征、残差连接、预训练和领域差异。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 `image-representation-convolution`。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。类比的 价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在 笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证 据。

3. 互动实验：只改变一个变量

实验 50-1 CNN、残差网络与迁移学习：单变量实验（教学模拟）

项目	内容
只改变量	冻结层比例，范围 0–100%，步长 5
实验目标	只改变“冻结层比例”，观察结果、代价和风险如何一起变化，理解理解层级特征、残差连接、预训练和领域差异。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把冻结层比例分别设为 0%、70%和 100%，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“冻结层比例”，观察结果、代价和风险如何一起变化，理解理解层级特征、残差连接、预训练和领域差异。

静态替代说明：静态替代：把冻结层比例分别设为 0%、70%和 100%，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $h_{l+1}=h_l+F(h_l)$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 50-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“CNN、残差网络与迁移学习”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解层级特征、残差连接、预训练和领域差异。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开道路网络与虚构出行任务建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园能源使用的匿名汇总数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“冻结层比例”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $h_{l+1}=h_l+F(h_l)$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、

空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开道路网络与虚构出行任务中，当冻结层比例变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“CNN、残差网络与迁移学习”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解层级特征、残差连接、预训练和领域差异。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开古诗文本与版权已明确的材料建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把不含个人信息的教学模拟天气记录作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“冻结层比例”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、

边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $h_{l+1}=h_l+F(h_l)$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开古诗文本与版权已明确的材料中，当冻结层比例变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“CNN、残差网络与迁移学习”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解层级特征、残差连接、预训练和领域差异。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开古诗文本与版权已明确的材料建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把不含个人信息的教学模拟天气记录作为迁移案例，检查相同表示和假设

是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“冻结层比例”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $h_{l+1}=h_l+F(h_l)$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开古诗文本与版权已明确的材料中，当冻结层比例变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“CNN、残差网络与迁移学习”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解层级特征、残差连接、预训练和领域差异。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开道路网络与虚构出行任务建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园能源使用的匿名汇总数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“冻结层比例”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $h_{l+1}=h_l+F(h_l)$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开道路网络与虚构出行任务中，当冻结层比例变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“CNN、残差网络与迁移学习”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解层级特征、残差连接、预训练和领域差异。。接着逐项标记观察到的事实、由公式推导的结果、来自文

献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开古诗文本与版权已明确的材料建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把不含个人信息的教学模拟天气记录作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“冻结层比例”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $h_{l+1}=h_l+F(h_l)$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开古诗文本与版权已明确的材料中，当冻结层比例变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“冻结层比例”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

35. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。

36. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。

37. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

38. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

39. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

40. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

41. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择公开道路网络与虚构出行任务作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择合成音频波形与环境声标签，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

42. **基础题：** 用自己的话解释“CNN、残差网络与迁移学习”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

43. **应用题：** 在虚构游戏角色的状态日志中设计一个只改变“冻结层比例”的实验，列出基线、三档设置、指标和失败样例。

44. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/cnn-resnet-transfer.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S026] Stanford University, 《CS231n: Deep Learning for Computer Vision》，[访问](https://cs231n.stanford.edu) cs231n.stanford.edu)
- [S027] Kaiming He et al., 《Deep Residual Learning for Image Recognition》，[访问](https://arxiv.org) arxiv.org)
- [S028] Alexey Dosovitskiy et al., 《An Image is Worth 16x16 Words》，[访问](https://arxiv.org) arxiv.org)
- [S071] Margaret Mitchell et al., 《Model Cards for Model Reporting》，[访问](https://arxiv.org) arxiv.org)

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 51 章 目标检测、分割与结构化输出

Detection and segmentation

项目	内容
学习单元	月 13 · 计算机视觉
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 50 章 CNN、残差网络与迁移学习

结论先行：区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“目标检测、分割与结构化输出”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 `cnn-resnet-transfer`。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 51-1 目标检测、分割与结构化输出：单变量实验（教学模拟）

项目	内容
只改变量	IoU 阈值，范围 0–1，步长 0.05
实验目标	只改变“IoU 阈值”，观察结果、代价和风险如何一起变化，理解区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把 IoU 阈值分别设为 0、0.5 和 1，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“IoU 阈值”，观察结果、代价和风险如何一起变化，理解区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。

静态替代说明：静态替代：把 IoU 阈值分别设为 0、0.5 和 1，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\text{IoU} = \text{area}(\text{AnB}) / \text{area}(\text{A} \cup \text{B})$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 51-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“目标检测、分割与结构化输出”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成的植物叶片特征建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开古诗文本与版权已明确的材料作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“IoU 阈值”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{IoU} = \text{area}(A \cap B) / \text{area}(A \cup B)$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、

极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成的植物叶片特征中，当 IoU 阈值变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“目标检测、分割与结构化输出”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构机器人在二维网格中的轨迹建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开道路网络与虚构出行任务作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“IoU 阈值”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $IoU = \text{area}(A \cap B) / \text{area}(A \cup B)$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在虚构机器人在二维网格中的轨迹中，当 IoU 阈值变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“目标检测、分割与结构化输出”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构机器人在二维网格中的轨迹建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开道路网络与虚构出行任务作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“IoU 阈值”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{IoU} = \text{area}(A \cap B) / \text{area}(A \cup B)$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在虚构机器人在二维网格中的轨迹中，当 IoU 阈值变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“目标检测、分割与结构化输出”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成的植物叶片特征建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均

值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开古诗文本与版权已明确的材料作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“IoU 阈值”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{IoU} = \text{area}(A \cap B) / \text{area}(A \cup B)$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成的植物叶片特征中，当 IoU 阈值变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“目标检测、分割与结构化输出”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳

定能力。照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构机器人在二维网格中的轨迹建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开道路网络与虚构出行任务作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“IoU 阈值”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{IoU} = \text{area}(A \cap B) / \text{area}(A \cup B)$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在虚构机器人在二维网格中的轨迹中，当 IoU 阈值变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“IoU 阈值”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

45. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
46. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
47. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

48. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

49. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

50. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

51. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择合成的植物叶片特征作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择校园能源使用的匿名汇总数据，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

52. **基础题：** 用自己的话解释“目标检测、分割与结构化输出”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

53. **应用题：** 在公开天文观测的缩小样例中设计一个只改变“IoU 阈值”的实验，列出基线、三档设置、指标和失败样例。

54. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/detection-segmentation.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S026] Stanford University, 《CS231n: Deep Learning for Computer Vision》，[访问 cs231n.stanford.edu](https://cs231n.stanford.edu))
- [S027] Kaiming He et al., 《Deep Residual Learning for Image Recognition》，[访问 arxiv.org](https://arxiv.org))
- [S028] Alexey Dosovitskiy et al., 《An Image is Worth 16x16 Words》，[访问 arxiv.org](https://arxiv.org))
- [S071] Margaret Mitchell et al., 《Model Cards for Model Reporting》，[访问 arxiv.org](https://arxiv.org))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 52 章 视觉 Transformer、生成视觉与评估

Vision transformers and evaluation

项目	内容
学习单元	月 13 · 计算机视觉
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：[第 51 章 目标检测、分割与结构化输出](#)

结论先行：理解图像分块、全局注意力、生成质量评估和数据偏见。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“视觉 Transformer、生成视觉与评估”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解图像分块、全局注意力、生成质量评估和数据偏见。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 detection-segmentation。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：把图像切成小方块当作视觉词元，让每块与其他块交换信息。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 52-1 视觉 Transformer、生成视觉与评估：单变量实验（教学模拟）

项目	内容
只改变量	图像块尺寸，范围 2–32px，步长 2
实验目标	只改变“图像块尺寸”，观察结果、代价和风险如何一起变化，理解理解图像分块、全局注意力、生成质量评估和数据偏见。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把图像块尺寸分别设为 2px、16px 和 32px，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“图像块尺寸”，观察结果、代价和风险如何一起变化，理解理解图像分块、全局注意力、生成质量评估和数据偏见。

静态替代说明：静态替代：把图像块尺寸分别设为 2px、16px 和 32px，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\text{attention}(Q, K, V) = \text{softmax}(QK^T/\sqrt{d})V$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 52-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“视觉 Transformer、生成视觉与评估”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解图像分块、全局注意力、生成质量评估和数据偏见。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把图像切成小方块当作视觉词元，让每块与其他块交换信息。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构游戏角色的状态日志建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构机器人在二维网格中的轨迹作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“图像块尺寸”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失

败样例。对于 $\text{attention}(Q,K,V)=\text{softmax}(QK^T/\sqrt{d})V$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把图像切成小方块当作视觉词元，让每块与其他块交换信息。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构游戏角色的状态日志中，当图像块尺寸变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“视觉 Transformer、生成视觉与评估”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解图像分块、全局注意力、生成质量评估和数据偏见。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把图像切成小方块当作视觉词元，让每块与其他块交换信息。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开科研论文的标题与摘要元数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成的植物叶片特征作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“图像块尺寸”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、

边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{attention}(Q,K,V)=\text{softmax}(QK^T/\sqrt{d})V$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把图像切成小方块当作视觉词元，让每块与其他块交换信息。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开科研论文的标题与摘要元数据中，当图像块尺寸变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“视觉 Transformer、生成视觉与评估”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解图像分块、全局注意力、生成质量评估和数据偏见。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把图像切成小方块当作视觉词元，让每块与其他块交换信息。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开科研论文的标题与摘要元数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，

最低可接受表现是什么？再把合成的植物叶片特征作为迁移案例，检查相同表示和假设是否仍成立。

若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“图像块尺寸”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{attention}(Q,K,V)=\text{softmax}(QK^T/\sqrt{d})V$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把图像切成小方块当作视觉词元，让每块与其他块交换信息。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开科研论文的标题与摘要元数据中，当图像块尺寸变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“视觉 Transformer、生成视觉与评估”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解图像分块、全局注意力、生成质量评估和数据偏见。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把图像切成小方块当作视觉词元，让每块与其他块交换信息。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构游戏角色的状态日志建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构机器人在二维网格中的轨迹作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“图像块尺寸”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{attention}(Q,K,V)=\text{softmax}(QK^T/\sqrt{d})V$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把图像切成小方块当作视觉词元，让每块与其他块交换信息。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构游戏角色的状态日志中，当图像块尺寸变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“视觉 Transformer、生成视觉与评估”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解图像分块、全局注意力、生成质量评估和数据偏见。。接着逐项标记观察到的事实、由公式推导

的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把图像切成小方块当作视觉词元，让每块与其他块交换信息。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开科研论文的标题与摘要元数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成的植物叶片特征作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“图像块尺寸”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{attention}(Q,K,V)=\text{softmax}(QK^T/\sqrt{d})V$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把图像切成小方块当作视觉词元，让每块与其他块交换信息。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开科研论文的标题与摘要元数据中，当图像块尺寸变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“图像块尺寸”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

55. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。

56. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。

57. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

58. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

59. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

60. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

61. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择虚构游戏角色的状态日志作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择公开古诗文本与版权已明确的材料，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

62. **基础题：** 用自己的话解释“视觉 Transformer、生成视觉与评估”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

63. **应用题：** 在合成音频波形与环境声标签中设计一个只改变“图像块尺寸”的实验，列出基线、三档设置、指标和失败样例。

64. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/vision-transformers-evaluation.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S026] Stanford University, 《CS231n: Deep Learning for Computer Vision》，[访问](https://cs231n.stanford.edu) cs231n.stanford.edu)
- [S027] Kaiming He et al., 《Deep Residual Learning for Image Recognition》，[访问](https://arxiv.org) arxiv.org)
- [S028] Alexey Dosovitskiy et al., 《An Image is Worth 16x16 Words》，[访问](https://arxiv.org) arxiv.org)
- [S071] Margaret Mitchell et al., 《Model Cards for Model Reporting》，[访问](https://arxiv.org) arxiv.org)

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

月 13 阶段项目：制作一个公开图像数据的可解释识别器

项目结论： 完成数据许可检查、增强、分类、混淆分析、显著性审查和 CPU 部署。当前状态为 draft。

交付物

- 问题与边界说明
- 可运行最小实现
- 实验记录与失败分析
- 来源与许可清单
- 风险、隐私与人工闸门
- 复现 README

验收方法

65. 在 CPU 或浏览器主线运行；若使用 GPU，另提供缩小数据冒烟测试。
66. 保存环境、依赖、随机种子、数据许可、测量记录和失败样例。
67. 逐条标记实际测量、教学模拟和文献引用，写清适用边界。
68. 不收集个人信息；高风险输出必须有人审阅、可拒答、可回滚。

第 53 章 文本、Unicode、分词与词元

Text and tokenization

项目	内容
学习单元	月 14 · 自然语言处理
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 52 章 [视觉 Transformer](#)、[生成视觉与评估](#)

结论先行：理解字符、字节、规范化、词、子词和词表外问题。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“文本、Unicode、分词与词元”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解字符、字节、规范化、词、子词和词表外问题。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 vision-transformers-evaluation。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：把一段话切成积木；切太大遇到新词，切太小序列变长。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 53-1 文本、Unicode、分词与词元：单变量实验（教学模拟）

项目	内容
只改变量	词表大小，范围 100–32000，步长 100
实验目标	只改变“词表大小”，观察结果、代价和风险如何一起变化，理解理解字符、字节、规范化、词、子词和词表外问题。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把词表大小分别设为 100、8000 和 32000，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“词表大小”，观察结果、代价和风险如何一起变化，理解理解字符、字节、规范化、词、子词和词表外问题。

静态替代说明：静态替代：把词表大小分别设为 100、8000 和 32000，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\text{text} \rightarrow \text{normalize} \rightarrow \text{tokens} \rightarrow \text{ids}$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 53-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“文本、Unicode、分词与词元”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解字符、字节、规范化、词、子词和词表外问题。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把一段话切成积木；切太大遇到新词，切太小序列变长。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开天文观测的缩小样例建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开科研论文的标题与摘要元数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“词表大小”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失

败样例。对于 $\text{text} \rightarrow \text{normalize} \rightarrow \text{tokens} \rightarrow \text{ids}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把一段话切成积木；切太大遇到新词，切太小序列变长。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开天文观测的缩小样例中，当词表大小变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“文本、Unicode、分词与词元”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解字符、字节、规范化、词、子词和词表外问题。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把一段话切成积木；切太大遇到新词，切太小序列变长。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成电商目录但不含真实用户行为建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构游戏角色的状态日志作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“词表大小”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 `text → normalize → tokens → ids`，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把一段话切成积木；切太大遇到新词，切太小序列变长。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成电商目录但不含真实用户行为中，当词表大小变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“文本、Unicode、分词与词元”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解字符、字节、规范化、词、子词和词表外问题。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把一段话切成积木；切太大遇到新词，切太小序列变长。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成电商目录但不含真实用户行为建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构游戏角色的状态日志作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“词表大小”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边

界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 `text` → `normalize` → `tokens` → `ids`，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把一段话切成积木；切太大遇到新词，切太小序列变长。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成电商目录但不含真实用户行为中，当词表大小变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“文本、Unicode、分词与词元”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解字符、字节、规范化、词、子词和词表外问题。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把一段话切成积木；切太大遇到新词，切太小序列变长。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开天文观测的缩小样例建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开科研论文的标题与摘要元数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“词表大小”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 `text → normalize → tokens → ids`，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把一段话切成积木；切太大遇到新词，切太小序列变长。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开天文观测的缩小样例中，当词表大小变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“文本、Unicode、分词与词元”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解字符、字节、规范化、词、子词和词表外问题。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把一段话切成积木；切太大遇到新词，切太小序列变长。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成电商目录但不含真实用户行为建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，

最低可接受表现是什么？再把虚构游戏角色的状态日志作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“词表大小”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 `text → normalize → tokens → ids`，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把一段话切成积木；切太大遇到新词，切太小序列变长。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成电商目录但不含真实用户行为中，当词表大小变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“词表大小”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

69. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。

70. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。

71. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

72. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

73. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

74. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

75. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择公开天文观测的缩小样例作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择虚构机器人在二维网格中的轨迹，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

76. **基础题**：用自己的话解释“文本、Unicode、分词与词元”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

77. **应用题**：在校园能源使用的匿名汇总数据中设计一个只改变“词表大小”的实验，列出基线、三档设置、指标和失败样例。

78. **挑战题**：设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/text-tokenization.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。

- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S029] Stanford University, 《CS224N: Natural Language Processing with Deep Learning》, [访问 web.stanford.edu](http://web.stanford.edu))
- [S030] Ashish Vaswani et al., 《Attention Is All You Need》, [访问 arxiv.org](http://arxiv.org))
- [S031] Jacob Devlin et al., 《BERT: Pre-training of Deep Bidirectional Transformers》, [访问 arxiv.org](http://arxiv.org))
- [S055] Patrick Lewis et al., 《Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks》, [访问 arxiv.org](http://arxiv.org))

核实日期：2026-08-06。评审状态：**draft**。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 54 章 词向量、RNN 与 LSTM

Embeddings, RNNs and LSTMs

项目	内容
学习单元	月 14 · 自然语言处理
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 53 章 文本、Unicode、分词与词元

结论先行：理解分布式表示、序列状态、长程依赖和门控记忆。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“词向量、RNN 与 LSTM”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解分布式表示、序列状态、长程依赖和门控记忆。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 text-tokenization。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。类比的價值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 54-1 词向量、RNN 与 LSTM：单变量实验（教学模拟）

项目	内容
只改变量	记忆保留率，范围 0–1，步长 0.05
实验目标	只改变“记忆保留率”，观察结果、代价和风险如何一起变化，理解理解分布式表示、序列状态、长程依赖和门控记忆。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把记忆保留率分别设为 0、0.8 和 1，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“记忆保留率”，观察结果、代价和风险如何一起变化，理解理解分布式表示、序列状态、长程依赖和门控记忆。

静态替代说明：静态替代：把记忆保留率分别设为 0、0.8 和 1，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $h_t = f(W_{xx}x_t + W_{hh}h_{t-1})$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 54-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“词向量、RNN 与 LSTM”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解分布式表示、序列状态、长程依赖和门控记忆。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成音频波形与环境声标签建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成电商目录但不含真实用户行为作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“记忆保留率”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $h_t = f(W_{xx_t} + W_{hh_{t-1}})$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、

极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成音频波形与环境声标签中，当记忆保留率变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“词向量、RNN 与 LSTM”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解分布式表示、序列状态、长程依赖和门控记忆。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园图书馆的公开借阅类别建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开天文观测的缩小样例作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“记忆保留率”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $h_t = f(W_{xx}x_t + W_{hh}h_{t-1})$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在校园图书馆的公开借阅类别中，当记忆保留率变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“词向量、RNN 与 LSTM”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解分布式表示、序列状态、长程依赖和门控记忆。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园图书馆的公开借阅类别建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开天文观测的缩小样例作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“记忆保留率”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $h_t = f(W_{xx}_t + W_{hh}_{t-1})$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在校园图书馆的公开借阅类别中，当记忆保留率变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“词向量、RNN 与 LSTM”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解分布式表示、序列状态、长程依赖和门控记忆。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成音频波形与环境声标签建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规

则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成电商目录但不含真实用户行为作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“记忆保留率”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $h_t = f(W_{xx_t} + W_{hh_{t-1}})$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成音频波形与环境声标签中，当记忆保留率变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“词向量、RNN 与 LSTM”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解分布式表示、序列状态、长程依赖和门控记忆。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。读

故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园图书馆的公开借阅类别建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开天文观测的缩小样例作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“记忆保留率”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $h_t = f(W_{xx}_t + W_{hh}_{t-1})$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在校园图书馆的公开借阅类别中，当记忆保留率变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“记忆保留率”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

79. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。

80. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。

81. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

82. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

83. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

84. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

85. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择合成音频波形与环境声标签作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择公开科研论文的标题与摘要元数据，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

86. **基础题：** 用自己的话解释“词向量、RNN 与 LSTM”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

87. **应用题：** 在公开古诗文本与版权已明确的材料中设计一个只改变“记忆保留率”的实验，列出基线、三档设置、指标和失败样例。

88. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/embeddings-rnn-lstm.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S029] Stanford University, 《CS224N: Natural Language Processing with Deep Learning》，[访问 web.stanford.edu](http://web.stanford.edu))
- [S030] Ashish Vaswani et al., 《Attention Is All You Need》，[访问 arxiv.org](http://arxiv.org))
- [S031] Jacob Devlin et al., 《BERT: Pre-training of Deep Bidirectional Transformers》，[访问 arxiv.org](http://arxiv.org))
- [S055] Patrick Lewis et al., 《Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks》，[访问 arxiv.org](http://arxiv.org))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 55 章 注意力与 Transformer

Attention and transformers

项目	内容
学习单元	月 14 · 自然语言处理
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：[第 54 章 词向量、RNN 与 LSTM](#)

结论先行：从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“注意力与 Transformer”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 embeddings-rnn-lstm。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：查资料时问题是查询，目录线索是键，找到的正文是值。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 55-1 注意力与 Transformer：单变量实验（教学模拟）

项目	内容
只改变量	注意力温度，范围 0.1–3，步长 0.1
实验目标	只改变“注意力温度”，观察结果、代价和风险如何一起变化，理解从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把注意力温度分别设为 0.1、1 和 3，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“注意力温度”，观察结果、代价和风险如何一起变化，理解从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。

静态替代说明：静态替代：把注意力温度分别设为 0.1、1 和 3，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $A = \text{softmax}(QK^T/\sqrt{d_k})V$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 55-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“注意力与 Transformer”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。查资料时问题是查询，目录线索是键，找到的正文是值。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园能源使用的匿名汇总数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园图书馆的公开借阅类别作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“注意力温度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $A = \text{softmax}(QK^T / \sqrt{d_k})V$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极

大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么查资料时问题是查询，目录线索是键，找到的正文是值。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园能源使用的匿名汇总数据中，当注意力温度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“注意力与 Transformer”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。查资料时问题是查询，目录线索是键，找到的正文是值。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用不含个人信息的教学模拟天气记录建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成音频波形与环境声标签作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“注意力温度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $A = \text{softmax}(QKT/\sqrt{d_k})V$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么查资料时问题是查询，目录线索是键，找到的正文是值。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在不含个人信息的教学模拟天气记录中，当注意力温度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“注意力与 Transformer”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。查资料时问题是查询，目录线索是键，找到的正文是值。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用不含个人信息的教学模拟天气记录建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成音频波形与环境声标签作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“注意力温度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $A = \text{softmax}(QKT/\sqrt{d_k})V$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么查资料时问题是查询，目录线索是键，找到的正文是值。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在不含个人信息的教学模拟天气记录中，当注意力温度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“注意力与 Transformer”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。查资料时问题是查询，目录线索是键，找到的正文是值。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园能源使用的匿名汇总数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规

则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园图书馆的公开借阅类别作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“注意力温度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $A = \text{softmax}(QK^T / \sqrt{d_k})V$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么查资料时问题是查询，目录线索是键，找到的正文是值。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在校园能源使用的匿名汇总数据中，当注意力温度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“注意力与 Transformer”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。查资料时问题是查询，目录线索是键，找到的正文是值。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用不含个人信息的教学模拟天气记录建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成音频波形与环境声标签作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“注意力温度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $A = \text{softmax}(QKT/\sqrt{d_k})V$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么查资料时问题是查询，目录线索是键，找到的正文是值。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在不含个人信息的教学模拟天气记录中，当注意力温度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和

`optimizer.step()`完成更新。评估阶段使用 `model.eval()`与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“注意力温度”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

89. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
90. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
91. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。
92. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。
93. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。
94. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。
95. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择校园能源使用的匿名汇总数据作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择合成电商目录但不含真实用户行为，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

96. **基础题：** 用自己的话解释“注意力与 Transformer”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。
97. **应用题：** 在虚构机器人在二维网格中的轨迹中设计一个只改变“注意力温度”的实验，列出基线、三档设置、指标和失败样例。
98. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/attention-transformer.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。

- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S029] Stanford University, 《CS224N: Natural Language Processing with Deep Learning》，[访问 web.stanford.edu](http://web.stanford.edu))
- [S030] Ashish Vaswani et al., 《Attention Is All You Need》，[访问 arxiv.org](http://arxiv.org))
- [S031] Jacob Devlin et al., 《BERT: Pre-training of Deep Bidirectional Transformers》，[访问 arxiv.org](http://arxiv.org))
- [S055] Patrick Lewis et al., 《Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks》，[访问 arxiv.org](http://arxiv.org))

核实日期：2026-08-06。评审状态：**draft**。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 56 章 NLP 任务、检索、评估与责任

NLP tasks, retrieval and evaluation

项目	内容
学习单元	月 14 · 自然语言处理
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系： [第 55 章 注意力与 Transformer](#)

结论先行： 覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。**版本边界：** 本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“NLP 任务、检索、评估与责任”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 attention-transformer。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 56-1 NLP 任务、检索、评估与责任：单变量实验（教学模拟）

项目	内容
只改变量	检索候选数，范围 1–30 条，步长 1
实验目标	只改变“检索候选数”，观察结果、代价和风险如何一起变化，理解覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把检索候选数分别设为 1 条、5 条和 30 条，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“检索候选数”，观察结果、代价和风险如何一起变化，理解覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。

静态替代说明：静态替代：把检索候选数分别设为 1 条、5 条和 30 条，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\text{score} = \text{relevance} + \text{faithfulness} + \text{utility} - \text{risk}$ 。先不要急着推公式。逐个给符

号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。

然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向 and 边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 56-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“NLP 任务、检索、评估与责任”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开古诗文本与版权已明确的材料建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把不含个人信息的教学模拟天气记录作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“检索候选数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{score} = \text{relevance} + \text{faithfulness} + \text{utility} - \text{risk}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开古诗文本与版权已明确的材料中，当检索候选数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“NLP 任务、检索、评估与责任”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开道路网络与虚构出行任务建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园能源使用的匿名汇总数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“检索候选数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{score} = \text{relevance} + \text{faithfulness} + \text{utility} - \text{risk}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开道路网络与虚构出行任务中，当检索候选数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“NLP 任务、检索、评估与责任”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开道路网络与虚构出行任务建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规

则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园能源使用的匿名汇总数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“检索候选数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{score} = \text{relevance} + \text{faithfulness} + \text{utility} - \text{risk}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开道路网络与虚构出行任务中，当检索候选数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“NLP 任务、检索、评估与责任”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳

定能力。一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开古诗文本与版权已明确的材料建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把不含个人信息的教学模拟天气记录作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“检索候选数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{score} = \text{relevance} + \text{faithfulness} + \text{utility} - \text{risk}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开古诗文本与版权已明确的材料中，当检索候选数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“NLP 任务、检索、评估与责任”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开道路网络与虚构出行任务建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园能源使用的匿名汇总数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“检索候选数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{score} = \text{relevance} + \text{faithfulness} + \text{utility} - \text{risk}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。只是入口，并给出一个类比失效的地方。如果解释中出现“肯

定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开道路网络与虚构出行任务中，当检索候选数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“检索候选数”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

- 99. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
- 100. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
- 101. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。
- 102. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。
- 103. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。
- 104. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。
- 105. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择公开古诗文本与版权已明确的材料作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择校园图书馆的公开借阅类别，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

- 106. **基础题：** 用自己的话解释“NLP 任务、检索、评估与责任”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

107. **应用题：**在公开科研论文的标题与摘要元数据中设计一个只改变“检索候选数”的实验，列出基线、三档设置、指标和失败样例。

108. **挑战题：**设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/nlp-tasks-retrieval-eval.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S029] Stanford University, 《CS224N: Natural Language Processing with Deep Learning》，[访问 web.stanford.edu](http://web.stanford.edu))
- [S030] Ashish Vaswani et al., 《Attention Is All You Need》，[访问 arxiv.org](http://arxiv.org))
- [S031] Jacob Devlin et al., 《BERT: Pre-training of Deep Bidirectional Transformers》，[访问 arxiv.org](http://arxiv.org))

- [S055] Patrick Lewis et al., 《Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks》, [访问 arxiv.org](#))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

月 14 阶段项目：做一个带检索证据的校园 FAQ 原型

项目结论：只使用公开校规或虚构资料，完成分词、检索、回答、引用、拒答和错误分析。当前状态为 draft。

交付物

- 问题与边界说明
- 可运行最小实现
- 实验记录与失败分析
- 来源与许可清单
- 风险、隐私与人工闸门
- 复现 README

验收方法

109. 在 CPU 或浏览器主线运行；若使用 GPU，另提供缩小数据冒烟测试。
110. 保存环境、依赖、随机种子、数据许可、测量记录和失败样例。
111. 逐条标记实际测量、教学模拟和文献引用，写清适用边界。
112. 不收集个人信息；高风险输出必须有人审阅、可拒答、可回滚。

第 57 章 波形、采样与短时傅里叶变换

Sampling and STFT

项目	内容
学习单元	月 15 · 语音与音频
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 56 章 NLP 任务、检索、评估与责任

结论先行：理解采样率、混叠、频率、相位、窗口和时频图。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“波形、采样与短时傅里叶变换”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解采样率、混叠、频率、相位、窗口和时频图。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 `nlp-tasks-retrieval-eval`。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 57-1 波形、采样与短时傅里叶变换：单变量实验（教学模拟）

项目	内容
只改变量	窗口长度，范围 64–2048 点，步长 64
实验目标	只改变“窗口长度”，观察结果、代价和风险如何一起变化，理解理解采样率、混叠、频率、相位、窗口和时频图。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把窗口长度分别设为 64 点、512 点和 2048 点，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“窗口长度”，观察结果、代价和风险如何一起变化，理解理解采样率、混叠、频率、相位、窗口和时频图。

静态替代说明：静态替代：把窗口长度分别设为 64 点、512 点和 2048 点，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $X(t, f) = \sum x[n]w[n-t]e^{-j2\pi fn}$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 57-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
```



```
loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
optimizer.zero_grad()
loss.backward()
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“波形、采样与短时傅里叶变换”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解采样率、混叠、频率、相位、窗口和时频图。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构机器人在二维网格中的轨迹建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开道路网络与虚构出行任务作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“窗口长度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $X(t,f)=\sum x[n]w[n-t]e^{-j2\pi fn}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构机器人在二维网格中的轨迹中，当窗口长度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“波形、采样与短时傅里叶变换”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解采样率、混叠、频率、相位、窗口和时频图。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成的植物叶片特征建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开古诗文本与版权已明确的材料作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“窗口长度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $X(t,f)=\sum x[n]w[n-t]e^{-j2\pi fn}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成的植物叶片特征中，当窗口长度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“波形、采样与短时傅里叶变换”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解采样率、混叠、频率、相位、窗口和时频图。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成的植物叶片特征建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均

值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开古诗文本与版权已明确的材料作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“窗口长度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $X(t,f)=\sum x[n]w[n-t]e^{-j2\pi fn}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成的植物叶片特征中，当窗口长度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“波形、采样与短时傅里叶变换”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解采样率、混叠、频率、相位、窗口和时频图。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。电影用

连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构机器人在二维网格中的轨迹建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开道路网络与虚构出行任务作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“窗口长度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $X(t,f)=\sum x[n]w[n-t]e^{-j2\pi fn}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构机器人在二维网格中的轨迹中，当窗口长度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“波形、采样与短时傅里叶变换”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解采样率、混叠、频率、相位、窗口和时频图。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成的植物叶片特征建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开古诗文本与版权已明确的材料作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“窗口长度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $X(t,f)=\sum x[n]w[n-t]e^{-j2\pi fn}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。只是入口，并给出一个类比失效的地方。如果解释中出

现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成的植物叶片特征中，当窗口长度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“窗口长度”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

- 113. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
- 114. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
- 115. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。
- 116. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。
- 117. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。
- 118. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。
- 119. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择虚构机器人在二维网格中的轨迹作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择不含个人信息的教学模拟天气记录，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

- 120. **基础题：** 用自己的话解释“波形、采样与短时傅里叶变换”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

121. **应用题：**在合成电商目录但不含真实用户行为中设计一个只改变“窗口长度”的实验，列出基线、三档设置、指标和失败样例。

122. **挑战题：**设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/sampling-stft.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S032] PyTorch, 《TorchAudio Documentation》, [访问 docs.pytorch.org](https://docs.pytorch.org))
- [S033] Awni Hannun et al., 《Deep Speech》, [访问 arxiv.org](https://arxiv.org))
- [S034] Aaron van den Oord et al., 《WaveNet》, [访问 arxiv.org](https://arxiv.org))

核实日期：2026-08-06。评审状态：**draft**。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 58 章 自动语音识别：声音到文字

Automatic speech recognition

项目	内容
学习单元	月 15 · 语音与音频
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系： [第 57 章 波形、采样与短时傅里叶变换](#)

结论先行： 理解声学表示、语言信息、CTC 或序列到序列和字错率。**版本边界：** 本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“自动语音识别：声音到文字”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解声学表示、语言信息、CTC 或序列到序列和字错率。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 `sampling-stft`。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：听写既要辨认声音，也会用句子上下文排除不合理词。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 58-1 自动语音识别：声音到文字：单变量实验（教学模拟）

项目	内容
只改变量	束搜索宽度，范围 1–20，步长 1
实验目标	只改变“束搜索宽度”，观察结果、代价和风险如何一起变化，理解理解声学表示、语言信息、CTC 或序列到序列和字错率。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把束搜索宽度分别设为 1、4 和 20，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“束搜索宽度”，观察结果、代价和风险如何一起变化，理解理解声学表示、语言信息、CTC 或序列到序列和字错率。

静态替代说明：静态替代：把束搜索宽度分别设为 1、4 和 20，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $WER=(S+D+I)/N$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 58-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“自动语音识别：声音到文字”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解声学表示、语言信息、CTC 或序列到序列和字错率。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。听写既要辨认声音，也会用句子上下文排除不合理词。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开科研论文的标题与摘要元数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成的植物叶片特征作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“束搜索宽度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $WER=(S+D+I)/N$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空

输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么听写既要辨认声音，也会用句子上下文排除不合理词。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开科研论文的标题与摘要元数据中，当束搜索宽度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“自动语音识别：声音到文字”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解声学表示、语言信息、CTC 或序列到序列和字错率。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。听写既要辨认声音，也会用句子上下文排除不合理词。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构游戏角色的状态日志建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构机器人在二维网格中的轨迹作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“束搜索宽度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $WER=(S+D+I)/N$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么听写既要辨认声音，也会用句子上下文排除不合理词。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在虚构游戏角色的状态日志中，当束搜索宽度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“自动语音识别：声音到文字”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解声学表示、语言信息、CTC 或序列到序列和字错率。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。听写既要辨认声音，也会用句子上下文排除不合理词。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构游戏角色的状态日志建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构机器人在二维网格中的轨迹作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“束搜索宽度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、

边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $WER=(S+D+I)/N$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么听写既要辨认声音，也会用句子上下文排除不合理词。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在虚构游戏角色的状态日志中，当束搜索宽度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“自动语音识别：声音到文字”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解声学表示、语言信息、CTC 或序列到序列和字错率。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。听写既要辨认声音，也会用句子上下文排除不合理词。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开科研论文的标题与摘要元数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成的植物叶片特征作为迁移案例，检查相同表示和假设是否仍成立。

若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“束搜索宽度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $WER=(S+D+I)/N$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么听写既要辨认声音，也会用句子上下文排除不合理词。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开科研论文的标题与摘要元数据中，当束搜索宽度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“自动语音识别：声音到文字”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解声学表示、语言信息、CTC 或序列到序列和字错率。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。听写既要辨认声音，也会用句子上下文排除不合理词。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构游戏角色的状态日志建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、

均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构机器人在二维网格中的轨迹作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“束搜索宽度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $WER=(S+D+I)/N$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么听写既要辨认声音，也会用句子上下文排除不合理词。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在虚构游戏角色的状态日志中，当束搜索宽度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“束搜索宽度”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

- 123. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
- 124. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
- 125. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。
- 126. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。
- 127. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。
- 128. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。
- 129. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择公开科研论文的标题与摘要元数据作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择公开道路网络与虚构出行任务，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

130. **基础题：**用自己的话解释“自动语音识别：声音到文字”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

131. **应用题：**在校园图书馆的公开借阅类别中设计一个只改变“束搜索宽度”的实验，列出基线、三档设置、指标和失败样例。

132. **挑战题：**设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/speech-recognition.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。

- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S032] PyTorch, 《TorchAudio Documentation》, [访问 docs.pytorch.org](https://docs.pytorch.org))
- [S033] Awni Hannun et al., 《Deep Speech》, [访问 arxiv.org](https://arxiv.org))
- [S034] Aaron van den Oord et al., 《WaveNet》, [访问 arxiv.org](https://arxiv.org))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 59 章 语音合成与声码器

Text to speech

项目	内容
学习单元	月 15 · 语音与音频
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：[第 58 章 自动语音识别：声音到文字](#)

结论先行：理解文本前端、声学模型、声码器、韵律和说话人控制的风险。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“语音合成与声码器”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解文本前端、声学模型、声码器、韵律和说话人控制的风险。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 speech-recognition。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 59-1 语音合成与声码器：单变量实验（教学模拟）

项目	内容
只改变量	采样温度，范围 0.1-2，步长 0.1
实验目标	只改变“采样温度”，观察结果、代价和风险如何一起变化，理解理解文本前端、声学模型、声码器、韵律和说话人控制的风险。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把采样温度分别设为 0.1、0.8 和 2，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“采样温度”，观察结果、代价和风险如何一起变化，理解理解文本前端、声学模型、声码器、韵律和说话人控制的风险。

静态替代说明：静态替代：把采样温度分别设为 0.1、0.8 和 2，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系：`text` → `acoustic features` → `waveform`。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 59-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```



```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化管理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“语音合成与声码器”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解文本前端、声学模型、声码器、韵律和说话人控制的风险。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成电商目录但不含真实用户行为建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构游戏角色的状态日志作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“采样温度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失

败样例。对于 text → acoustic features → waveform，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成电商目录但不含真实用户行为中，当采样温度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“语音合成与声码器”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解文本前端、声学模型、声码器、韵律和说话人控制的风险。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开天文观测的缩小样例建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开科研论文的标题与摘要元数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“采样温度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边

界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 `text → acoustic features → waveform`，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开天文观测的缩小样例中，当采样温度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“语音合成与声码器”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解文本前端、声学模型、声码器、韵律和说话人控制的风险。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开天文观测的缩小样例建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接

受表现是什么？再把公开科研论文的标题与摘要元数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“采样温度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 `text` → `acoustic features` → `waveform`，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开天文观测的缩小样例中，当采样温度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“语音合成与声码器”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解文本前端、声学模型、声码器、韵律和说话人控制的风险。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成电商目录但不含真实用户行为建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构游戏角色的状态日志作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“采样温度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{text} \rightarrow \text{acoustic features} \rightarrow \text{waveform}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成电商目录但不含真实用户行为中，当采样温度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“语音合成与声码器”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解文本前端、声学模型、声码器、韵律和说话人控制的风险。。接着逐项标记观察到的事实、由公式推导的结果、来

自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开天文观测的缩小样例建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开科研论文的标题与摘要元数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“采样温度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 `text → acoustic features → waveform`，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开天文观测的缩小样例中，当采样温度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“采样温度”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

133. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
134. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
135. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

136. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

137. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

138. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

139. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择合成电商目录但不含真实用户行为作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择合成的植物叶片特征，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

140. **基础题：** 用自己的话解释“语音合成与声码器”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

141. **应用题：** 在不含个人信息的教学模拟天气记录中设计一个只改变“采样温度”的实验，列出基线、三档设置、指标和失败样例。

142. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/speech-synthesis.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S032] PyTorch, 《TorchAudio Documentation》, [访问 docs.pytorch.org](https://docs.pytorch.org))
- [S033] Awni Hannun et al., 《Deep Speech》, [访问 arxiv.org](https://arxiv.org))
- [S034] Aaron van den Oord et al., 《WaveNet》, [访问 arxiv.org](https://arxiv.org))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 60 章 音频理解、音乐与说话人隐私

Audio understanding and privacy

项目	内容
学习单元	月 15 · 语音与音频
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 59 章 语音合成与声码器

结论先行：覆盖事件检测、音乐表示、说话人识别与匿名化边界。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“音频理解、音乐与说话人隐私”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：覆盖事件检测、音乐表示、说话人识别与匿名化边界。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 speech-synthesis。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 60-1 音频理解、音乐与说话人隐私：单变量实验（教学模拟）

项目	内容
只改变量	隐私预算，范围 0.1–10 ϵ ，步长 0.1
实验目标	只改变“隐私预算”，观察结果、代价和风险如何一起变化，理解覆盖事件检测、音乐表示、说话人识别与匿名化边界。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把隐私预算分别设为 0.1 ϵ 、1 ϵ 和 10 ϵ ，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“隐私预算”，观察结果、代价和风险如何一起变化，理解覆盖事件检测、音乐表示、说话人识别与匿名化边界。

静态替代说明：静态替代：把隐私预算分别设为 0.1ϵ 、 1ϵ 和 10ϵ ，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\text{risk} = \text{identifiability} \times \text{exposure} \times \text{consequence}$ 。先不要急着推公式。逐个给符号

贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 60-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“音频理解、音乐与说话人隐私”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：覆盖事件检测、音乐表示、说话人识别与匿名化边界。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园图书馆的公开借阅类别建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开天文观测的缩小样例作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“隐私预算”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失

败样例。对于 $\text{risk} = \text{identifiability} \times \text{exposure} \times \text{consequence}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园图书馆的公开借阅类别中，当隐私预算变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“音频理解、音乐与说话人隐私”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：覆盖事件检测、音乐表示、说话人识别与匿名化边界。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成音频波形与环境声标签建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成电商目录但不含真实用户行为作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“隐私预算”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边

界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{risk} = \text{identifiability} \times \text{exposure} \times \text{consequence}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成音频波形与环境声标签中，当隐私预算变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“音频理解、音乐与说话人隐私”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：覆盖事件检测、音乐表示、说话人识别与匿名化边界。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成音频波形与环境声标签建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低

可接受表现是什么？再把合成电商目录但不含真实用户行为作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“隐私预算”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{risk} = \text{identifiability} \times \text{exposure} \times \text{consequence}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成音频波形与环境声标签中，当隐私预算变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“音频理解、音乐与说话人隐私”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：覆盖事件检测、音乐表示、说话人识别与匿名化边界。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园图书馆的公开借阅类别建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开天文观测的缩小样例作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“隐私预算”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{risk} = \text{identifiability} \times \text{exposure} \times \text{consequence}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在校园图书馆的公开借阅类别中，当隐私预算变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“音频理解、音乐与说话人隐私”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：覆盖事件检测、音乐表示、说话人识别与匿名化边界。。接着逐项标记观察到的事实、由公式推导的结果、

来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成音频波形与环境声标签建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成电商目录但不含真实用户行为作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“隐私预算”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{risk} = \text{identifiability} \times \text{exposure} \times \text{consequence}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成音频波形与环境声标签中，当隐私预算变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“隐私预算”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

143. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
144. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
145. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

146. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

147. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

148. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

149. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择校园图书馆的公开借阅类别作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择虚构游戏角色的状态日志，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

150. **基础题：** 用自己的话解释“音频理解、音乐与说话人隐私”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

151. **应用题：** 在公开道路网络与虚构出行任务中设计一个只改变“隐私预算”的实验，列出基线、三档设置、指标和失败样例。

152. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/audio-understanding-privacy.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S032] PyTorch, 《TorchAudio Documentation》, [访问 docs.pytorch.org](https://docs.pytorch.org))
- [S033] Awni Hannun et al., 《Deep Speech》, [访问 arxiv.org](https://arxiv.org))
- [S034] Aaron van den Oord et al., 《WaveNet》, [访问 arxiv.org](https://arxiv.org))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

月 15 阶段项目：制作一个不上传声音的本地音频分类实验

项目结论： 使用公开音频或合成波形，完成采样、频谱、分类、噪声测试和隐私说明。当前状态为 draft。

交付物

- 问题与边界说明
- 可运行最小实现
- 实验记录与失败分析
- 来源与许可清单
- 风险、隐私与人工闸门
- 复现 README

验收方法

153. 在 CPU 或浏览器主线运行；若使用 GPU，另提供缩小数据冒烟测试。
154. 保存环境、依赖、随机种子、数据许可、测量记录和失败样例。
155. 逐条标记实际测量、教学模拟和文献引用，写清适用边界。
156. 不收集个人信息；高风险输出必须有人审阅、可拒答、可回滚。

第 61 章 生成建模与变分自编码器

Generative modeling and VAEs

项目	内容
学习单元	月 16 · 生成模型、扩散与流模型
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：[第 60 章 音频理解、音乐与说话人隐私](#)

结论先行： 区分显式、隐式生成，理解潜变量、重参数化和证据下界。**版本边界：** 本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“生成建模与变分自编码器”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：区分显式、隐式生成，理解潜变量、重参数化和证据下界。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 `audio-understanding-privacy`。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：把复杂图像压进一张连续地图，再从地图附近采样重建新图案。类比的值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 61-1 生成建模与变分自编码器：单变量实验（教学模拟）

项目	内容
只改变量	潜变量维度，范围 2–128，步长 2
实验目标	只改变“潜变量维度”，观察结果、代价和风险如何一起变化，理解区分显式、隐式生成，理解潜变量、重参数化和证据下界。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把潜变量维度分别设为 2、16 和 128，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“潜变量维度”，观察结果、代价和风险如何一起变化，理解区分显式、隐式生成，理解潜变量、重参数化和证据下界。

静态替代说明：静态替代：把潜变量维度分别设为 2、16 和 128，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $ELBO = E_q[\log p(x|z)] - D_{KL}(q(z|x) || p(z))$ 。先不要急着推公式。逐个给符号贴标签：

它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 61-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化管理理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“生成建模与变分自编码器”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分显式、隐式生成，理解潜变量、重参数化和证据下界。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把复杂图像压进一张连续地图，再从地图附近采样重建新图案。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用不含个人信息的教学模拟天气记录建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成音频波形与环境声标签作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“潜变量维度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失

败样例。对于 $ELBO = E_q[\log p(x|z)] - D_{KL}(q(z|x)||p(z))$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把复杂图像压进一张连续地图，再从地图附近采样重建新图案。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在不含个人信息的教学模拟天气记录中，当潜变量维度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“生成建模与变分自编码器”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分显式、隐式生成，理解潜变量、重参数化和证据下界。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把复杂图像压进一张连续地图，再从地图附近采样重建新图案。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园能源使用的匿名汇总数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园图书馆的公开借阅类别作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“潜变量维度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、

边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $ELBO = E_q[\log p(x|z)] - D_{KL}(q(z|x)||p(z))$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把复杂图像压进一张连续地图，再从地图附近采样重建新图案。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在校园能源使用的匿名汇总数据中，当潜变量维度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“生成建模与变分自编码器”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分显式、隐式生成，理解潜变量、重参数化和证据下界。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把复杂图像压进一张连续地图，再从地图附近采样重建新图案。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园能源使用的匿名汇总数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低

可接受表现是什么？再把校园图书馆的公开借阅类别作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“潜变量维度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $ELBO = E_q[\log p(x|z)] - D_{KL}(q(z|x)||p(z))$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把复杂图像压进一张连续地图，再从地图附近采样重建新图案。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在校园能源使用的匿名汇总数据中，当潜变量维度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“生成建模与变分自编码器”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分显式、隐式生成，理解潜变量、重参数化和证据下界。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把复杂图像压进一张连续地图，再从地图附近采样重建新图案。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用不含个人信息的教学模拟天气记录建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成音频波形与环境声标签作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“潜变量维度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $ELBO = E_q[\log p(x|z)] - D_{KL}(q(z|x)||p(z))$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把复杂图像压进一张连续地图，再从地图附近采样重建新图案。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在不含个人信息的教学模拟天气记录中，当潜变量维度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“生成建模与变分自编码器”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分显式、隐式生成，理解潜变量、重参数化和证据下界。。接着逐项标记观察到的事实、由公式推导的结果、

来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把复杂图像压进一张连续地图，再从地图附近采样重建新图案。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园能源使用的匿名汇总数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园图书馆的公开借阅类别作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“潜变量维度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $ELBO = E_q[\log p(x|z)] - D_{KL}(q(z|x)||p(z))$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把复杂图像压进一张连续地图，再从地图附近采样重建新图案。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在校园能源使用的匿名汇总数据中，当潜变量维度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“潜变量维度”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

157. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
158. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
159. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

160. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

161. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

162. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

163. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择不含个人信息的教学模拟天气记录作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择公开天文观测的缩小样例，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

164. **基础题：** 用自己的话解释“生成建模与变分自编码器”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

165. **应用题：** 在合成的植物叶片特征中设计一个只改变“潜变量维度”的实验，列出基线、三档设置、指标和失败样例。

166. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/generative-models-vae.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S035] Diederik P. Kingma, Max Welling, 《Auto-Encoding Variational Bayes》，[访问 arxiv.org](#))
- [S036] Ian Goodfellow et al., 《Generative Adversarial Nets》，[访问 arxiv.org](#))
- [S037] Jonathan Ho et al., 《Denoising Diffusion Probabilistic Models》，[访问 arxiv.org](#))
- [S038] Yang Song et al., 《Score-Based Generative Modeling through Stochastic Differential Equations》，[访问 arxiv.org](#))
- [S039] Yaron Lipman et al., 《Flow Matching for Generative Modeling》，[访问 arxiv.org](#))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 62 章 生成对抗网络

Generative adversarial networks

项目	内容
学习单元	月 16 · 生成模型、扩散与流模型
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 61 章 [生成建模与变分自编码器](#)

结论先行：理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“生成对抗网络”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 `generative-models-vae`。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 62-1 生成对抗网络：单变量实验（教学模拟）

项目	内容
只改变量	判别器步数，范围 1–10 步，步长 1
实验目标	只改变“判别器步数”，观察结果、代价和风险如何一起变化，理解理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把判别器步数分别设为 1 步、1 步和 10 步，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“判别器步数”，观察结果、代价和风险如何一起变化，理解理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。

静态替代说明：静态替代：把判别器步数分别设为 1 步、1 步和 10 步，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\min_G \max_D E[\log D(x)] + E[\log(1 - D(G(z)))]$ 。先不要急着推公式。逐个给符号贴标签：

它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 62-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“生成对抗网络”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开道路网络与虚构出行任务建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园能源使用的匿名汇总数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“判别器步数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失

败样例。对于 $\min_G \max_D E[\log D(x)] + E[\log(1-D(G(z)))]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开道路网络与虚构出行任务中，当判别器步数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“生成对抗网络”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开古诗文本与版权已明确的材料建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把不含个人信息的教学模拟天气记录作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“判别器步数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、

边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\min_G \max_D E[\log D(x)] + E[\log(1 - D(G(z)))]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开古诗文本与版权已明确的材料中，当判别器步数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“生成对抗网络”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开古诗文本与版权已明确的材料建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把不含个人信息的教学模拟天气记录作为迁移案例，检查相同表示和假设

是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“判别器步数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\min_G \max_D E[\log D(x)] + E[\log(1 - D(G(z)))]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开古诗文本与版权已明确的材料中，当判别器步数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“生成对抗网络”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开道路网络与虚构出行任务建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园能源使用的匿名汇总数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“判别器步数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\min_G \max_D E[\log D(x)] + E[\log(1 - D(G(z)))]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开道路网络与虚构出行任务中，当判别器步数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“生成对抗网络”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。。接着逐项标记观察到的事实、由公式推导的结果、来自文献

的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开古诗文本与版权已明确的材料建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把不含个人信息的教学模拟天气记录作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“判别器步数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\min_G \max_D E[\log D(x)] + E[\log(1 - D(G(z)))]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开古诗文本与版权已明确的材料中，当判别器步数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“判别器步数”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

167. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
168. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
169. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

170. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

171. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

172. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

173. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择公开道路网络与虚构出行任务作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择合成音频波形与环境声标签，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

174. **基础题：** 用自己的话解释“生成对抗网络”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

175. **应用题：** 在虚构游戏角色的状态日志中设计一个只改变“判别器步数”的实验，列出基线、三档设置、指标和失败样例。

176. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 content/ai-book/answers/gan.md，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S035] Diederik P. Kingma, Max Welling, 《Auto-Encoding Variational Bayes》, [访问 arxiv.org](#))
- [S036] Ian Goodfellow et al., 《Generative Adversarial Nets》, [访问 arxiv.org](#))
- [S037] Jonathan Ho et al., 《Denoising Diffusion Probabilistic Models》, [访问 arxiv.org](#))
- [S038] Yang Song et al., 《Score-Based Generative Modeling through Stochastic Differential Equations》, [访问 arxiv.org](#))
- [S039] Yaron Lipman et al., 《Flow Matching for Generative Modeling》, [访问 arxiv.org](#))

核实日期：2026-08-06。评审状态：**draft**。只有技术评审、事实核查和专家签字完成后，状态才能按 **draft** → **technical_review** → **fact_checked** → **stable** 前进。

第 63 章 扩散模型与分数匹配

Diffusion and score models

项目	内容
学习单元	月 16 · 生成模型、扩散与流模型
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：[第 62 章 生成对抗网络](#)

结论先行：理解加噪、去噪、分数函数、采样步数和条件引导。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“扩散模型与分数匹配”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解加噪、去噪、分数函数、采样步数和条件引导。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 gan。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 63-1 扩散模型与分数匹配：单变量实验（教学模拟）

项目	内容
只改变量	去噪步数，范围 5–1000 步，步长 5
实验目标	只改变“去噪步数”，观察结果、代价和风险如何一起变化，理解理解加噪、去噪、分数函数、采样步数和条件引导。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把去噪步数分别设为 5 步、50 步和 1000 步，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“去噪步数”，观察结果、代价和风险如何一起变化，理解理解加噪、去噪、分数函数、采样步数和条件引导。

静态替代说明：静态替代：把去噪步数分别设为 5 步、50 步和 1000 步，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $x_t = \sqrt{\alpha_t} x_0 + \sqrt{(1-\alpha_t)}\epsilon$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 63-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“扩散模型与分数匹配”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解加噪、去噪、分数函数、采样步数和条件引导。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成的植物叶片特征建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开古诗文本与版权已明确的材料作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“去噪步数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $x_t = \sqrt{\alpha_t} x_0 + \sqrt{(1-\alpha_t)} \epsilon$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、

极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成的植物叶片特征中，当去噪步数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“扩散模型与分数匹配”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解加噪、去噪、分数函数、采样步数和条件引导。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构机器人在二维网格中的轨迹建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开道路网络与虚构出行任务作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“去噪步数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $x_t = \sqrt{\alpha_t} x_0 + \sqrt{(1-\alpha_t)} \epsilon$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构机器人在二维网格中的轨迹中，当去噪步数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“扩散模型与分数匹配”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解加噪、去噪、分数函数、采样步数和条件引导。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构机器人在二维网格中的轨迹建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开道路网络与虚构出行任务作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“去噪步数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $x_t = \sqrt{\alpha_t} x_0 + \sqrt{(1-\alpha_t)} \epsilon$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构机器人在二维网格中的轨迹中，当去噪步数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“扩散模型与分数匹配”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解加噪、去噪、分数函数、采样步数和条件引导。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成的植物叶片特征建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均

值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开古诗文本与版权已明确的材料作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“去噪步数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $x_t = \sqrt{\alpha_t} x_0 + \sqrt{(1-\alpha_t)}\epsilon$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成的植物叶片特征中，当去噪步数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“扩散模型与分数匹配”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解加噪、去噪、分数函数、采样步数和条件引导。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构机器人在二维网格中的轨迹建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开道路网络与虚构出行任务作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“去噪步数”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $x_t = \sqrt{\alpha_t} x_0 + \sqrt{(1-\alpha_t)} \epsilon$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构机器人在二维网格中的轨迹中，当去噪步数变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和

`optimizer.step()`完成更新。评估阶段使用 `model.eval()`与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“去噪步数”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

177. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
178. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
179. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。
180. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。
181. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。
182. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。
183. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择合成的植物叶片特征作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择校园能源使用的匿名汇总数据，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

184. **基础题：**用自己的话解释“扩散模型与分数匹配”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

185. **应用题：**在公开天文观测的缩小样例中设计一个只改变“去噪步数”的实验，列出基线、三档设置、指标和失败样例。

186. **挑战题：**设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/diffusion-score.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。

- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S035] Diederik P. Kingma, Max Welling, 《Auto-Encoding Variational Bayes》, [访问 arxiv.org](#))
- [S036] Ian Goodfellow et al., 《Generative Adversarial Nets》, [访问 arxiv.org](#))
- [S037] Jonathan Ho et al., 《Denoising Diffusion Probabilistic Models》, [访问 arxiv.org](#))
- [S038] Yang Song et al., 《Score-Based Generative Modeling through Stochastic Differential Equations》, [访问 arxiv.org](#))
- [S039] Yaron Lipman et al., 《Flow Matching for Generative Modeling》, [访问 arxiv.org](#))

核实日期：2026-08-06。评审状态：**draft**。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 64 章 流模型、能量模型与生成评估

Flows, energy models and evaluation

项目	内容
学习单元	月 16 · 生成模型、扩散与流模型
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 63 章 [扩散模型与分数匹配](#)

结论先行：理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“流模型、能量模型与生成评估”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 diffusion-score。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 64-1 流模型、能量模型与生成评估：单变量实验（教学模拟）

项目	内容
只改变量	引导强度，范围 0–20，步长 0.5
实验目标	只改变“引导强度”，观察结果、代价和风险如何一起变化，理解理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把引导强度分别设为 0、7.5 和 20，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“引导强度”，观察结果、代价和风险如何一起变化，理解理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。

静态替代说明：静态替代：把引导强度分别设为 0、7.5 和 20，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\log p_x(x) = \log p_z(f(x)) + \log |\det J_f(x)|$ 。先不要急着推公式。逐个给符号贴标签：

它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 64-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“流模型、能量模型与生成评估”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构游戏角色的状态日志建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构机器人在二维网格中的轨迹作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“引导强度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失

败样例。对于 $\log p_x(x) = \log p_z(f(x)) + \log |\det J_f(x)|$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在虚构游戏角色的状态日志中，当引导强度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“流模型、能量模型与生成评估”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开科研论文的标题与摘要元数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成的植物叶片特征作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“引导强度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边

界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\log p_x(x) = \log p_z(f(x)) + \log |\det J_f(x)|$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开科研论文的标题与摘要元数据中，当引导强度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“流模型、能量模型与生成评估”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开科研论文的标题与摘要元数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，

最低可接受表现是什么？再把合成的植物叶片特征作为迁移案例，检查相同表示和假设是否仍成立。

若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“引导强度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\log p_x(x) = \log p_z(f(x)) + \log |\det J_f(x)|$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开科研论文的标题与摘要元数据中，当引导强度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“流模型、能量模型与生成评估”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构游戏角色的状态日志建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构机器人在二维网格中的轨迹作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“引导强度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\log p_x(x) = \log p_z(f(x)) + \log |\det J_f(x)|$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在虚构游戏角色的状态日志中，当引导强度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“流模型、能量模型与生成评估”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。。接着逐项标记观察到的事实、由公式推导

的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开科研论文的标题与摘要元数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成的植物叶片特征作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“引导强度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\log p_x(x) = \log p_z(f(x)) + \log |\det J_f(x)|$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开科研论文的标题与摘要元数据中，当引导强度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“引导强度”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

187. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
188. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
189. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

- 190. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。
- 191. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。
- 192. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。
- 193. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择虚构游戏角色的状态日志作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择公开古诗文本与版权已明确的材料，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

- 194. **基础题：** 用自己的话解释“流模型、能量模型与生成评估”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。
- 195. **应用题：** 在合成音频波形与环境声标签中设计一个只改变“引导强度”的实验，列出基线、三档设置、指标和失败样例。
- 196. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/flows-energy-evaluation.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S035] Diederik P. Kingma, Max Welling, 《Auto-Encoding Variational Bayes》，[访问 arxiv.org](#)
- [S036] Ian Goodfellow et al., 《Generative Adversarial Nets》，[访问 arxiv.org](#)
- [S037] Jonathan Ho et al., 《Denoising Diffusion Probabilistic Models》，[访问 arxiv.org](#)
- [S038] Yang Song et al., 《Score-Based Generative Modeling through Stochastic Differential Equations》，[访问 arxiv.org](#)
- [S039] Yaron Lipman et al., 《Flow Matching for Generative Modeling》，[访问 arxiv.org](#)

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

月 16 阶段项目：生成并审计一组教学模拟图案

项目结论：比较 VAE、GAN、扩散或流的玩具实现，记录模式覆盖、质量、成本、许可和滥用风险。当前状态为 draft。

交付物

- 问题与边界说明
- 可运行最小实现
- 实验记录与失败分析
- 来源与许可清单
- 风险、隐私与人工闸门
- 复现 README

验收方法

197. 在 CPU 或浏览器主线运行；若使用 GPU，另提供缩小数据冒烟测试。
198. 保存环境、依赖、随机种子、数据许可、测量记录和失败样例。
199. 逐条标记实际测量、教学模拟和文献引用，写清适用边界。
200. 不收集个人信息；高风险输出必须有人审阅、可拒答、可回滚。

第 65 章 MDP、回报与贝尔曼方程

MDPs and Bellman equations

项目	内容
学习单元	月 17 · 强化学习与控制
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系： [第 64 章 流模型、能量模型与生成评估](#)

结论先行： 理解状态、动作、转移、奖励、折扣和马尔可夫假设。**版本边界：** 本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“MDP、回报与贝尔曼方程”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解状态、动作、转移、奖励、折扣和马尔可夫假设。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 flows-energy-evaluation。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 65-1 MDP、回报与贝尔曼方程：单变量实验（教学模拟）

项目	内容
只改变量	折扣因子，范围 0–1 γ ，步长 0.01
实验目标	只改变“折扣因子”，观察结果、代价和风险如何一起变化，理解理解状态、动作、转移、奖励、折扣和马尔可夫假设。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把折扣因子分别设为 0 γ 、0.95 γ 和 1 γ ，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性

项目	内容
	能或现实世界因果效果。

实验目标：只改变“折扣因子”，观察结果、代价和风险如何一起变化，理解理解状态、动作、转移、奖励、折扣和马尔可夫假设。

静态替代说明：静态替代：把折扣因子分别设为 0γ 、 0.95γ 和 1γ ，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $V^{\pi}(s)=E[r+\gamma V^{\pi}(s')|s]$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 65-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
```

```

)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})

```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“MDP、回报与贝尔曼方程”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解状态、动作、转移、奖励、折扣和马尔可夫假设。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开天文观测的缩小样例建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开科研论文的标题与摘要元数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“折扣因子”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $V^\pi(s) = E[r + \gamma V^\pi(s') | s]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开天文观测的缩小样例中，当折扣因子变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“MDP、回报与贝尔曼方程”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解状态、动作、转移、奖励、折扣和马尔可夫假设。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成电商目录但不含真实用户行为建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构游戏角色的状态日志作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“折扣因子”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $V^{\pi}(s) = E[r + \gamma V^{\pi}(s') | s]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成电商目录但不含真实用户行为中，当折扣因子变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“MDP、回报与贝尔曼方程”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解状态、动作、转移、奖励、折扣和马尔可夫假设。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成电商目录但不含真实用户行为建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如

固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构游戏角色的状态日志作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“折扣因子”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $V^{\pi}(s) = E[r + \gamma V^{\pi}(s') | s]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成电商目录但不含真实用户行为中，当折扣因子变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“MDP、回报与贝尔曼方程”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解状态、动作、转移、奖励、折扣和马尔可夫假设。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。走迷宫

时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开天文观测的缩小样例建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开科研论文的标题与摘要元数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“折扣因子”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $V^{\pi}(s) = E[r + \gamma V^{\pi}(s') | s]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开天文观测的缩小样例中，当折扣因子变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“MDP、回报与贝尔曼方程”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解状态、动作、转移、奖励、折扣和马尔可夫假设。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成电商目录但不含真实用户行为建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构游戏角色的状态日志作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“折扣因子”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $V^{\pi}(s) = E[r + \gamma V^{\pi}(s') | s]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。只是入口，并给出一个类比失效的地方。如果解释中出

现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成电商目录但不含真实用户行为中，当折扣因子变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“折扣因子”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

- 201. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
- 202. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
- 203. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。
- 204. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。
- 205. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。
- 206. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。
- 207. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择公开天文观测的缩小样例作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择虚构机器人在二维网格中的轨迹，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

- 208. **基础题：**用自己的话解释“MDP、回报与贝尔曼方程”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

209. **应用题：** 在校园能源使用的匿名汇总数据中设计一个只改变“折扣因子”的实验，列出基线、三档设置、指标和失败样例。

210. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/mdp-bellman.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S040] Richard Sutton, Andrew Barto, 《Reinforcement Learning: An Introduction》，[访问 incompleteideas.net](https://incompleteideas.net))
- [S041] UC Berkeley, 《CS 285: Deep Reinforcement Learning》，[访问 rail.eecs.berkeley.edu](https://rail.eecs.berkeley.edu))
- [S042] Volodymyr Mnih et al., 《Human-level control through deep reinforcement learning》，[访问 doi.org](https://doi.org))
- [S043] John Schulman et al., 《Proximal Policy Optimization Algorithms》，[访问 arxiv.org](https://arxiv.org))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 66 章 价值学习、Q-learning 与 DQN

Value learning and DQN

项目	内容
学习单元	月 17 · 强化学习与控制
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 65 章 MDP、回报与贝尔曼方程

结论先行： 从时序差分更新到经验回放、目标网络和过估计问题。**版本边界：** 本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“价值学习、Q-learning 与 DQN”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：从时序差分更新到经验回放、目标网络和过估计问题。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 mdp-bellman。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。类比的值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 66-1 价值学习、Q-learning 与 DQN：单变量实验（教学模拟）

项目	内容
只改变量	探索率，范围 $0-1\epsilon$ ，步长 0.05
实验目标	只改变“探索率”，观察结果、代价和风险如何一起变化，理解从时序差分更新到经验回放、目标网络和过估计问题。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把探索率分别设为 0ϵ 、 0.2ϵ 和 1ϵ ，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“探索率”，观察结果、代价和风险如何一起变化，理解从时序差分更新到经验回放、目标网络和过估计问题。

静态替代说明：静态替代：把探索率分别设为 0ϵ 、 0.2ϵ 和 1ϵ ，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $Q \leftarrow Q + \alpha[r + \gamma \max_{Q'} Q - Q]$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 66-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“价值学习、Q-learning 与 DQN”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：从时序差分更新到经验回放、目标网络和过估计问题。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成音频波形与环境声标签建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成电商目录但不含真实用户行为作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“探索率”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $Q \leftarrow Q + \alpha[r + \gamma \max_{Q'} Q - Q]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极

大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成音频波形与环境声标签中，当探索率变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“价值学习、Q-learning 与 DQN”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：从时序差分更新到经验回放、目标网络和过估计问题。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园图书馆的公开借阅类别建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开天文观测的缩小样例作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“探索率”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $Q \leftarrow Q + \alpha[r + \gamma \max_{Q'} Q - Q]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园图书馆的公开借阅类别中，当探索率变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“价值学习、Q-learning 与 DQN”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：从时序差分更新到经验回放、目标网络和过估计问题。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园图书馆的公开借阅类别建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开天文观测的缩小样例作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“探索率”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $Q \leftarrow Q + \alpha[r + \gamma \max_{Q'} Q - Q]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园图书馆的公开借阅类别中，当探索率变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“价值学习、Q-learning 与 DQN”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：从时序差分更新到经验回放、目标网络和过估计问题。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成音频波形与环境声标签建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规

则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成电商目录但不含真实用户行为作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“探索率”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $Q \leftarrow Q + \alpha[r + \gamma \max_{Q'} Q' - Q]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成音频波形与环境声标签中，当探索率变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“价值学习、Q-learning 与 DQN”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：从时序差分更新到经验回放、目标网络和过估计问题。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成

稳定能力。学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园图书馆的公开借阅类别建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开天文观测的缩小样例作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“探索率”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $Q \leftarrow Q + \alpha[r + \gamma \max_{a'} Q' - Q]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园图书馆的公开借阅类别中，当探索率变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“探索率”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

211. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
212. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
213. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

214. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

215. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

216. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

217. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择合成音频波形与环境声标签作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择公开科研论文的标题与摘要元数据，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

218. **基础题：** 用自己的话解释“价值学习、Q-learning 与 DQN”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

219. **应用题：** 在公开古诗文本与版权已明确的材料中设计一个只改变“探索率”的实验，列出基线、三档设置、指标和失败样例。

220. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/q-learning-dqn.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S040] Richard Sutton, Andrew Barto, 《Reinforcement Learning: An Introduction》，[访问 incompleteideas.net](https://incompleteideas.net))
- [S041] UC Berkeley, 《CS 285: Deep Reinforcement Learning》，[访问 rail.eecs.berkeley.edu](https://rail.eecs.berkeley.edu))
- [S042] Volodymyr Mnih et al., 《Human-level control through deep reinforcement learning》，[访问 doi.org](https://doi.org))
- [S043] John Schulman et al., 《Proximal Policy Optimization Algorithms》，[访问 arxiv.org](https://arxiv.org))

核实日期：2026-08-06。评审状态：**draft**。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 67 章 策略梯度、Actor-Critic 与 PPO

Policy gradients and PPO

项目	内容
学习单元	月 17 · 强化学习与控制
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：[第 66 章 价值学习、Q-learning 与 DQN](#)

结论先行：直接优化策略概率，用价值基线降方差，理解裁剪目标。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“策略梯度、Actor-Critic 与 PPO”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：直接优化策略概率，用价值基线降方差，理解裁剪目标。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 q-learning-dqn。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 67-1 策略梯度、Actor-Critic 与 PPO：单变量实验（教学模拟）

项目	内容
只改变量	裁剪范围，范围 0.05–0.5，步长 0.05
实验目标	只改变“裁剪范围”，观察结果、代价和风险如何一起变化，理解直接优化策略概率，用价值基线降方差，理解裁剪目标。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把裁剪范围分别设为 0.05、0.2 和 0.5，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“裁剪范围”，观察结果、代价和风险如何一起变化，理解直接优化策略概率，用价值基线降方差，理解裁剪目标。

静态替代说明：静态替代：把裁剪范围分别设为 0.05、0.2 和 0.5，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\nabla J = E[\nabla \log \pi(a|s)]$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 67-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“策略梯度、Actor-Critic 与 PPO”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：直接优化策略概率，用价值基线降方差，理解裁剪目标。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园能源使用的匿名汇总数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园图书馆的公开借阅类别作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“裁剪范围”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\nabla J = E[\nabla \log \pi(a|s)\hat{A}]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、

空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园能源使用的匿名汇总数据中，当裁剪范围变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“策略梯度、Actor-Critic 与 PPO”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：直接优化策略概率，用价值基线降方差，理解裁剪目标。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用不含个人信息的教学模拟天气记录建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成音频波形与环境声标签作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“裁剪范围”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\nabla J = E[\nabla \log \pi(a|s)]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在不含个人信息的教学模拟天气记录中，当裁剪范围变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“策略梯度、Actor-Critic 与 PPO”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：直接优化策略概率，用价值基线降方差，理解裁剪目标。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用不含个人信息的教学模拟天气记录建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成音频波形与环境声标签作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“裁剪范围”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\nabla J = E[\nabla \log \pi(a|s)]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在不含个人信息的教学模拟天气记录中，当裁剪范围变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“策略梯度、Actor-Critic 与 PPO”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：直接优化策略概率，用价值基线降方差，理解裁剪目标。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园能源使用的匿名汇总数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规

则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园图书馆的公开借阅类别作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“裁剪范围”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\nabla J = E[\nabla \log \pi(a|s)]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园能源使用的匿名汇总数据中，当裁剪范围变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“策略梯度、Actor-Critic 与 PPO”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：直接优化策略概率，用价值基线降方差，理解裁剪目标。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成

稳定能力。演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用不含个人信息的教学模拟天气记录建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成音频波形与环境声标签作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“裁剪范围”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\nabla J = E[\nabla \log \pi(a|s)]$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在不含个人信息的教学模拟天气记录中，当裁剪范围变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“裁剪范围”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

221. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
222. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
223. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

224. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

225. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

226. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

227. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择校园能源使用的匿名汇总数据作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择合成电商目录但不含真实用户行为，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

228. **基础题：** 用自己的话解释“策略梯度、Actor-Critic 与 PPO”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

229. **应用题：** 在虚构机器人在二维网格中的轨迹中设计一个只改变“裁剪范围”的实验，列出基线、三档设置、指标和失败样例。

230. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/policy-gradient-ppo.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S040] Richard Sutton, Andrew Barto, 《Reinforcement Learning: An Introduction》，[访问 incompleteideas.net](https://incompleteideas.net))
- [S041] UC Berkeley, 《CS 285: Deep Reinforcement Learning》，[访问 rail.eecs.berkeley.edu](https://rail.eecs.berkeley.edu))
- [S042] Volodymyr Mnih et al., 《Human-level control through deep reinforcement learning》，[访问 doi.org](https://doi.org))
- [S043] John Schulman et al., 《Proximal Policy Optimization Algorithms》，[访问 arxiv.org](https://arxiv.org))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 68 章 模型式、离线、多智能体与安全 RL

Model-based, offline and safe RL

项目	内容
学习单元	月 17 · 强化学习与控制
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：[第 67 章 策略梯度、Actor-Critic 与 PPO](#)

结论先行：理解环境模型、分布外动作、信用分配、约束和安全探索。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“模型式、离线、多智能体与安全 RL”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解环境模型、分布外动作、信用分配、约束和安全探索。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 policy-gradient-ppo。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 68-1 模型式、离线、多智能体与安全 RL：单变量实验（教学模拟）

项目	内容
只改变量	分布偏移，范围 0–100%，步长 5
实验目标	只改变“分布偏移”，观察结果、代价和风险如何一起变化，理解理解环境模型、分布外动作、信用分配、约束和安全探索。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把分布偏移分别设为 0%、25%和 100%，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“分布偏移”，观察结果、代价和风险如何一起变化，理解理解环境模型、分布外动作、信用分配、约束和安全探索。

静态替代说明：静态替代：把分布偏移分别设为 0%、25%和 100%，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\text{maximize } E[\text{return}] \text{ subject to } E[\text{cost}] \leq \text{limit}$ 。先不要急着推公式。逐个给符号贴标

签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 68-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化管理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“模型式、离线、多智能体与安全 RL”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解环境模型、分布外动作、信用分配、约束和安全探索。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开古诗文本与版权已明确的材料建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把不含个人信息的教学模拟天气记录作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“分布偏移”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{maximize } E[\text{return}] \text{ subject to } E[\text{cost}] \leq \text{limit}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开古诗文本与版权已明确的材料中，当分布偏移变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“模型式、离线、多智能体与安全 RL”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解环境模型、分布外动作、信用分配、约束和安全探索。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开道路网络与虚构出行任务建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园能源使用的匿名汇总数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“分布偏移”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{maximize } E[\text{return}] \text{ subject to } E[\text{cost}] \leq \text{limit}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开道路网络与虚构出行任务中，当分布偏移变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“模型式、离线、多智能体与安全 RL”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解环境模型、分布外动作、信用分配、约束和安全探索。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开道路网络与虚构出行任务建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规

则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园能源使用的匿名汇总数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“分布偏移”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{maximize } E[\text{return}] \text{ subject to } E[\text{cost}] \leq \text{limit}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开道路网络与虚构出行任务中，当分布偏移变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“模型式、离线、多智能体与安全 RL”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解环境模型、分布外动作、信用分配、约束和安全探索。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能

力。只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开古诗文本与版权已明确的材料建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把不含个人信息的教学模拟天气记录作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“分布偏移”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{maximize } E[\text{return}] \text{ subject to } E[\text{cost}] \leq \text{limit}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开古诗文本与版权已明确的材料中，当分布偏移变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“模型式、离线、多智能体与安全 RL”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解环境模型、分布外动作、信用分配、约束和安全探索。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开道路网络与虚构出行任务建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把校园能源使用的匿名汇总数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“分布偏移”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{maximize } E[\text{return}] \text{ subject to } E[\text{cost}] \leq \text{limit}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完

全” “智能” “理解” 等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开道路网络与虚构出行任务中，当分布偏移变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“分布偏移”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

- 231. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
- 232. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
- 233. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。
- 234. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。
- 235. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。
- 236. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。
- 237. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择公开古诗文本与版权已明确的材料作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择校园图书馆的公开借阅类别，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

- 238. **基础题：** 用自己的话解释“模型式、离线、多智能体与安全 RL”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

239. **应用题：**在公开科研论文的标题与摘要元数据中设计一个只改变“分布偏移”的实验，列出基线、三档设置、指标和失败样例。

240. **挑战题：**设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/model-based-offline-safe-rl.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S040] Richard Sutton, Andrew Barto, 《Reinforcement Learning: An Introduction》，[访问 incompleteideas.net](https://incompleteideas.net))
- [S041] UC Berkeley, 《CS 285: Deep Reinforcement Learning》，[访问 rail.eecs.berkeley.edu](https://rail.eecs.berkeley.edu))
- [S042] Volodymyr Mnih et al., 《Human-level control through deep reinforcement learning》，[访问 doi.org](https://doi.org))
- [S043] John Schulman et al., 《Proximal Policy Optimization Algorithms》，[访问 arxiv.org](https://arxiv.org))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

月 17 阶段项目：训练一个可解释的网格世界智能体

项目结论：用教学模拟环境记录奖励、策略、探索、种子、学习曲线和失败轨迹，不把单次成功当结论。当前状态为 draft。

交付物

- 问题与边界说明
- 可运行最小实现
- 实验记录与失败分析
- 来源与许可清单
- 风险、隐私与人工闸门
- 复现 README

验收方法

241. 在 CPU 或浏览器主线运行；若使用 GPU，另提供缩小数据冒烟测试。
242. 保存环境、依赖、随机种子、数据许可、测量记录和失败样例。
243. 逐条标记实际测量、教学模拟和文献引用，写清适用边界。
244. 不收集个人信息；高风险输出必须有人审阅、可拒答、可回滚。

第 69 章 坐标、运动学与动力学

Kinematics and dynamics

项目	内容
学习单元	月 18 · 机器人与具身智能
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：[第 68 章 模型式、离线、多智能体与安全 RL](#)

结论先行：理解坐标系、位姿、关节、正逆运动学、速度与力。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“坐标、运动学与动力学”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解坐标系、位姿、关节、正逆运动学、速度与力。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 model-based-offline-safe-rl。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 69-1 坐标、运动学与动力学：单变量实验（教学模拟）

项目	内容
只改变量	关节角度，范围 -180–180°，步长 5
实验目标	只改变“关节角度”，观察结果、代价和风险如何一起变化，理解理解坐标系、位姿、关节、正逆运动学、速度与力。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把关节角度分别设为-180°、0°和 180°，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“关节角度”，观察结果、代价和风险如何一起变化，理解理解坐标系、位姿、关节、正逆运动学、速度与力。

静态替代说明：静态替代：把关节角度分别设为-180°、0°和 180°，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $x=f(q)$ ； $\dot{x}=J(q)\dot{q}$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。

若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 69-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“坐标、运动学与动力学”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解坐标系、位姿、关节、正逆运动学、速度与力。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构机器人在二维网格中的轨迹建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开道路网络与虚构出行任务作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“关节角度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $x=f(q)$ ； $\dot{x}=J(q)\dot{q}$ ；逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空

输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构机器人在二维网格中的轨迹中，当关节角度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“坐标、运动学与动力学”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解坐标系、位姿、关节、正逆运动学、速度与力。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成的植物叶片特征建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开古诗文本与版权已明确的材料作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“关节角度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $x=f(q)$; $x=J(q)q'$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成的植物叶片特征中，当关节角度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“坐标、运动学与动力学”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解坐标系、位姿、关节、正逆运动学、速度与力。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成的植物叶片特征建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开古诗文本与版权已明确的材料作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“关节角度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边

界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $x=f(q)$; $\dot{x}=J(q)q$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成的植物叶片特征中，当关节角度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“坐标、运动学与动力学”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解坐标系、位姿、关节、正逆运动学、速度与力。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构机器人在二维网格中的轨迹建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开道路网络与虚构出行任务作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“关节角度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $x=f(q)$; $\dot{x}=J(q)\dot{q}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构机器人在二维网格中的轨迹中，当关节角度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“坐标、运动学与动力学”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解坐标系、位姿、关节、正逆运动学、速度与力。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成的植物叶片特征建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均

值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开古诗文本与版权已明确的材料作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“关节角度”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $x=f(q)$; $x=J(q)q$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在合成的植物叶片特征中，当关节角度变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“关节角度”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

- 245. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
- 246. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
- 247. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。
- 248. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。
- 249. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。
- 250. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。
- 251. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择虚构机器人在二维网格中的轨迹作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择不含个人信息的教学模拟天气记录，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

252. **基础题：** 用自己的话解释“坐标、运动学与动力学”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

253. **应用题：** 在合成电商目录但不含真实用户行为中设计一个只改变“关节角度”的实验，列出基线、三档设置、指标和失败样例。

254. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/kinematics-dynamics.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。

- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S017] Stanford University, 《CS221: Artificial Intelligence》, [访问 stanford-cs221.github.io](https://stanford-cs221.github.io))
- [S044] Open Robotics, 《ROS 2 Documentation》, [访问 docs.ros.org](https://docs.ros.org))
- [S045] Sebastian Thrun, Wolfram Burgard, Dieter Fox, 《Probabilistic Robotics》, [访问 mitpress.mit.edu](https://mitpress.mit.edu))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 70 章 传感、定位、地图与 SLAM

Sensing, localization and SLAM

项目	内容
学习单元	月 18 · 机器人与具身智能
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 69 章 [坐标、运动学与动力学](#)

结论先行：融合带噪观测，在未知环境同时估计位姿与地图。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“传感、定位、地图与 SLAM”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：融合带噪观测，在未知环境同时估计位姿与地图。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 kinematics-dynamics。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。类比的值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 70-1 传感、定位、地图与 SLAM：单变量实验（教学模拟）

项目	内容
只改变量	传感噪声，范围 0–100%，步长 5
实验目标	只改变“传感噪声”，观察结果、代价和风险如何一起变化，理解融合带噪观测，在未知环境同时估计位姿与地图。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把传感噪声分别设为 0%、10%和 100%，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“传感噪声”，观察结果、代价和风险如何一起变化，理解融合带噪观测，在未知环境同时估计位姿与地图。

静态替代说明：静态替代：把传感噪声分别设为 0%、10% 和 100%，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\text{belief}(x_t) \propto p(z_t|x_t) \int p(x_t|u_t, x_{t-1}) \text{belief}(x_{t-1}) dx$ 。先不要急着推公式。

逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 70-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“传感、定位、地图与 SLAM”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：融合带噪观测，在未知环境同时估计位姿与地图。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开科研论文的标题与摘要元数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成的植物叶片特征作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“传感噪声”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失

败样例。对于 $\text{belief}(x_t) \propto p(z_t|x_t) \int p(x_t|u_t, x_{t-1}) \text{belief}(x_{t-1}) dx$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开科研论文的标题与摘要元数据中，当传感噪声变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“传感、定位、地图与 SLAM”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：融合带噪观测，在未知环境同时估计位姿与地图。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构游戏角色的状态日志建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构机器人在二维网格中的轨迹作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“传感噪声”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边

界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{belief}(x_t) \propto p(z_t|x_t) \int p(x_t|u_t, x_{t-1}) \text{belief}(x_{t-1}) dx$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构游戏角色的状态日志中，当传感噪声变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“传感、定位、地图与 SLAM”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：融合带噪观测，在未知环境同时估计位姿与地图。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构游戏角色的状态日志建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构机器人在二维网格中的轨迹作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“传感噪声”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{belief}(x_t) \propto p(z_t|x_t) \int p(x_t|u_t, x_{t-1}) \text{belief}(x_{t-1}) dx$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构游戏角色的状态日志中，当传感噪声变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“传感、定位、地图与 SLAM”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：融合带噪观测，在未知环境同时估计位姿与地图。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开科研论文的标题与摘要元数据建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，

最低可接受表现是什么？再把合成的植物叶片特征作为迁移案例，检查相同表示和假设是否仍成立。

若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“传感噪声”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{belief}(x_t) \propto p(z_t|x_t) \int p(x_t|u_t, x_{t-1}) \text{belief}(x_{t-1}) dx$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在公开科研论文的标题与摘要元数据中，当传感噪声变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“传感、定位、地图与 SLAM”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：融合带噪观测，在未知环境同时估计位姿与地图。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用虚构游戏角色的状态日志建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构机器人在二维网格中的轨迹作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“传感噪声”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{belief}(x_t) \propto p(z_t|x_t) \int p(x_t|u_t, x_{t-1}) \text{belief}(x_{t-1}) dx$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它替换成可观察行为和适用条件。最后写一句研究问题：在虚构游戏角色的状态日志中，当传感噪声变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存

`state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“传感噪声”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

255. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
256. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
257. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。
258. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。
259. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。
260. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。
261. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择公开科研论文的标题与摘要元数据作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择公开道路网络与虚构出行任务，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

262. **基础题：**用自己的话解释“传感、定位、地图与 SLAM”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

263. **应用题：**在校园图书馆的公开借阅类别中设计一个只改变“传感噪声”的实验，列出基线、三档设置、指标和失败样例。

264. **挑战题：**设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/sensing-slam.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。

- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S017] Stanford University, 《CS221: Artificial Intelligence》，[访问 stanford-cs221.github.io](https://stanford-cs221.github.io))
- [S044] Open Robotics, 《ROS 2 Documentation》，[访问 docs.ros.org](https://docs.ros.org))
- [S045] Sebastian Thrun, Wolfram Burgard, Dieter Fox, 《Probabilistic Robotics》，[访问 mitpress.mit.edu](https://mitpress.mit.edu))

核实日期：2026-08-06。评审状态：draft。只有技术评审、事实核查和专家签字完成后，状态才能按 draft → technical_review → fact_checked → stable 前进。

第 71 章 运动规划与反馈控制

Motion planning and control

项目	内容
学习单元	月 18 · 机器人与具身智能
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 70 章 传感、定位、地图与 SLAM

结论先行： 区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。**版本边界：** 本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“运动规划与反馈控制”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 sensing-slam。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 71-1 运动规划与反馈控制：单变量实验（教学模拟）

项目	内容
只改变量	比例增益，范围 0–10Kp，步长 0.1
实验目标	只改变“比例增益”，观察结果、代价和风险如何一起变化，理解区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把比例增益分别设为 0Kp、1Kp 和 10Kp，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“比例增益”，观察结果、代价和风险如何一起变化，理解区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。

静态替代说明：静态替代：把比例增益分别设为 0Kp、1Kp 和 10Kp，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $u_t = K_p e_t + K_i \Sigma e + K_d \Delta e$ 。先不要急着推公式。逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 71-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
    optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“运动规划与反馈控制”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成电商目录但不含真实用户行为建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构游戏角色的状态日志作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“比例增益”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $u_t = K_p e_t + K_i \sum e + K_d \Delta e$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、

极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成电商目录但不含真实用户行为中，当比例增益变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“运动规划与反馈控制”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开天文观测的缩小样例建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开科研论文的标题与摘要元数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“比例增益”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $u_t = K_p e_t + K_i \sum e + K_d \Delta e$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开天文观测的缩小样例中，当比例增益变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“运动规划与反馈控制”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开天文观测的缩小样例建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开科研论文的标题与摘要元数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“比例增益”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $u_t = K_p e_t + K_i \Sigma e + K_d \Delta e$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开天文观测的缩小样例中，当比例增益变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“运动规划与反馈控制”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成电商目录但不含真实用户行为建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如

固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把虚构游戏角色的状态日志作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“比例增益”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $u_t = K_p e_t + K_i \Sigma e + K_d \Delta e$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成电商目录但不含真实用户行为中，当比例增益变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“运动规划与反馈控制”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能

力。导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用公开天文观测的缩小样例建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开科研论文的标题与摘要元数据作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“比例增益”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $u_t = K_p e_t + K_i \Sigma e + K_d \Delta e$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在公开天文观测的缩小样例中，当比例增益变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“比例增益”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

265. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
266. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
267. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

268. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

269. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

270. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

271. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择合成电商目录但不含真实用户行为作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择合成的植物叶片特征，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

272. **基础题：** 用自己的话解释“运动规划与反馈控制”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

273. **应用题：** 在不含个人信息的教学模拟天气记录中设计一个只改变“比例增益”的实验，列出基线、三档设置、指标和失败样例。

274. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/motion-planning-control.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S017] Stanford University, 《CS221: Artificial Intelligence》，[访问 stanford-cs221.github.io](https://stanford-cs221.github.io))
- [S044] Open Robotics, 《ROS 2 Documentation》，[访问 docs.ros.org](https://docs.ros.org))
- [S045] Sebastian Thrun, Wolfram Burgard, Dieter Fox, 《Probabilistic Robotics》，[访问 mitpress.mit.edu](https://mitpress.mit.edu))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

第 72 章 机器人学习、仿真到现实与人身安全

Robot learning and sim-to-real

项目	内容
学习单元	月 18 · 机器人与具身智能
建议时间	8 小时
评审状态	draft · 核实 2026-08-06
练习与实验	3 道练习 · 1 个互动实验

先修关系：第 71 章 [运动规划与反馈控制](#)

结论先行：理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。**版本边界：**本章属于 2026.08 Beta，评审状态为 draft。它是可运行、可核查的教学稿，不等于专家签字后的正式版。

1. 为什么重要，现在能做什么

学完本章，你应该能把“机器人学习、仿真到现实与人身安全”从一个名词变成可操作的分析框架。你能解释它在完整 AI 系统中的位置，写出最小数学关系，运行一个 CPU 可承受的示例，设计只改变一个变量的实验，识别至少三种失败原因，并把方法迁移到新的公开或虚构场景。真正的能力不是复述答案，而是面对结果不理想时知道先检查哪里、需要补什么证据、何时应该拒绝继续自动化。

本章聚焦：理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。这件事重要，因为 AI 系统的错误通常不是“模型突然不聪明”，而是问题定义、数据表示、目标函数、评估或部署条件之间不一致。把这些环节分开，才能定位故障，也才能对他人解释为什么一个结果值得或不值得相信。

2. 先修检查与生活类比

先用一分钟自测：你能否说明输入和输出分别是什么？能否区分规则、算法、模型与系统？能否读懂变量、函数和简单图表？如果其中一项还不稳，先回到前置章节 motion-planning-control。不要跳过地基；后续章节默认你会保存代码、记录环境、保护隐私，并区分教学模拟与真实测量。

生活类比：飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。类比的价值是帮助你先获得方向感，但它会省略重要细节。本章后面会用数学、代码和反例修正直觉。请在笔记里写下类比对对应关系，并额外写一条“类比失效处”；这一步能防止把好记的故事误当成严谨证据。

3. 互动实验：只改变一个变量

实验 72-1 机器人学习、仿真到现实与人身安全：单变量实验（教学模拟）

项目	内容
只改变量	现实差距，范围 0–100%，步长 5
实验目标	只改变“现实差距”，观察结果、代价和风险如何一起变化，理解理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。
键盘操作	聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。
静态替代	静态替代：把现实差距分别设为 0%、20%和 100%，手工比较三组教学模拟输出。
结果边界	页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

实验目标：只改变“现实差距”，观察结果、代价和风险如何一起变化，理解理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。

静态替代说明：静态替代：把现实差距分别设为 0%、20%和 100%，手工比较三组教学模拟输出。

键盘操作：聚焦滑块后使用方向键微调，Page Up/Page Down 大步调整，Home/End 到达边界。

风险提示：页面数值由公开公式生成，只用于教学，不代表真实模型性能或现实世界因果效果。

4. 直觉到数学

核心关系： $\text{deployment gap} = \text{real_distribution} - \text{simulator_distribution}$ 。先不要急着推公式。

逐个给符号贴标签：它表示现实中的什么对象、是标量还是向量、单位是什么、允许取什么范围、由谁测量。然后用最小数字手算一次，再交给代码。若手算、代码和图形不一致，优先检查单位、索引、符号方向和边界，而不是马上换模型。

数学的作用不是让内容显得困难，而是把模糊说法变成可检查关系。公式必须和任务定义相互约束：

如果目标变化，损失和指标也可能需要变化；如果数据尺度变化，数值稳定性和优化速度也可能变化；

如果输出被用于真实决策，还必须把错误代价、拒答和人工复核写进系统。

5. 最小实现

下面代码保留固定种子和“教学模拟”标签。它的目的不是刷新榜单，而是让你看到输入、状态、计算和输出怎样连接。真实项目要补充数据许可、环境文件、独立测试、异常处理和测量记录。

代码 72-1 python 最小实现

```
import torch

torch.manual_seed(20260806)
x = torch.randn(16, 4)
y = (x.sum(dim=1, keepdim=True) > 0).float()
model = torch.nn.Sequential(
    torch.nn.Linear(4, 8),
    torch.nn.ReLU(),
    torch.nn.Linear(8, 1),
)
optimizer = torch.optim.AdamW(model.parameters(), lr=1e-2)
for _ in range(40):
    loss = torch.nn.functional.binary_cross_entropy_with_logits(model(x), y)
    optimizer.zero_grad()
    loss.backward()
```

```
optimizer.step()
print({"loss": round(loss.item(), 4), "seed": 20260806})
```

运行后先检查输出类型、范围和极端值，再改变一个参数。不要一次改很多行；每次改变都记录“我预期什么、实际发生什么、可能原因是什么”。如果缺少 PyTorch，可先完成浏览器互动实验和纯 Python 主线；GPU 只属于后续研究复现轨道。

6. 五轮系统化理解

1. 问题边界

先把要解决的任务写成输入、输出、约束、失败代价与不做什么。对“机器人学习、仿真到现实与人身安全”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园图书馆的公开借阅类别建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开天文观测的缩小样例作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“现实差距”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失

败样例。对于 $\text{deployment gap} = \text{real_distribution} - \text{simulator_distribution}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园图书馆的公开借阅类别中，当现实差距变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

3. 机制与因果链

沿着数据进入、内部计算、输出形成和外部行动逐步追踪，而不是只记名词。对“机器人学习、仿真到现实与人身安全”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成音频波形与环境声标签建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成电商目录但不含真实用户行为作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“现实差距”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边

界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{deployment gap} = \text{real_distribution} - \text{simulator_distribution}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成音频波形与环境声标签中，当现实差距变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. 评估与不确定性

把平均指标拆成切片、置信区间、校准、错误代价和最坏情况。对“机器人学习、仿真到现实与人身安全”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成音频波形与环境声标签建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低

可接受表现是什么？再把合成电商目录但不含真实用户行为作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“现实差距”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{deployment gap} = \text{real_distribution} - \text{simulator_distribution}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成音频波形与环境声标签中，当现实差距变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

9. 工程与复现

固定版本、环境、种子和测量记录，使别人能从原始输入重建结论。对“机器人学习、仿真到现实与人身安全”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。。接着逐项标记观察到的事实、由公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用校园图书馆的公开借阅类别建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把公开天文观测的缩小样例作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“现实差距”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{deployment gap} = \text{real_distribution} - \text{simulator_distribution}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在校园图书馆的公开借阅类别中，当现实差距变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

11. 迁移与研究

把本章方法搬到新情境，用对照和消融判断哪些部分可迁移、哪些需要重做。对“机器人学习、仿真到现实与人身安全”而言，第一步不是背下定义，而是把核心问题写成一句能被反驳、能被测量的话：理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。。接着逐项标记观察到的事实、由

公式推导的结果、来自文献的结论和仍然不确定的部分。这样做能防止把界面效果、单个案例或流畅文字误当成稳定能力。飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。这个类比只帮助建立直觉，不能代替形式定义；当类比与公式冲突时，以经过核实的定义、实验和边界为准。

先用合成音频波形与环境声标签建立最小案例。只保留一个输入、一个可解释的中间量和一个输出，写清数据是“教学模拟”还是“实际测量”。然后建立一个不使用本章复杂方法的基线，例如固定规则、均值、随机策略或人工清单。基线不是为了显得简单，而是为了回答：如果什么都不优化，最低可接受表现是什么？再把合成电商目录但不含真实用户行为作为迁移案例，检查相同表示和假设是否仍成立。若必须改变数据定义、损失或评价标准，就把改变记录为新的实验条件，而不是悄悄调整。

本层实验只调节“现实差距”。先预测它变小时结果、成本和风险会怎样，再移动滑块核对教学模拟曲线。至少记录低、中、高三个点，不能只保留最好看的点。若曲线与预测不符，依次排查单位、边界、符号方向、初始化、随机性和实现。若曲线符合预测，也不能直接声称现实有效：页面只验证公式在简化条件下的行为，真实结论仍需要代表性数据、独立测试和部署观察。

常见错误是一次同时改变数据、模型和阈值，最后无法知道改进来自哪里。正确做法是建立实验矩阵：行表示唯一改变的变量，列记录假设、设置、种子、运行环境、主要指标、切片指标、资源成本和失败样例。对于 $\text{deployment gap} = \text{real_distribution} - \text{simulator_distribution}$ ，逐个说明符号的对象、形状、单位和取值范围；把零值、极大值、空输入、重复输入和相反方向代入，检查是否符合直觉。任何无法解释的异常都应保留在失败日志，而不是删除。

完成本层的标准不是“看懂了”，而是你能不看正文讲出三件事：本章方法解决什么问题；它依赖哪些假设；怎样设计一个能让它失败的测试。再向同学解释为什么飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。只是入口，并给出一个类比失效的地方。如果解释中出现“肯定”“完全”“智能”“理解”等宽泛词，就把它们替换成可观察行为和适用条件。最后写一句研究问题：在合成音频波形与环境声标签中，当现实差距变化时，哪个机制最可能先成为瓶颈，怎样用对照实验验证？

7. PyTorch 实现路线

当本章涉及学习模型时，统一采用 Python 与 PyTorch：先把输入变成带明确形状的张量，再定义 `torch.nn.Module`，选择与任务一致的损失，使用 `optimizer.zero_grad()`、`loss.backward()` 和 `optimizer.step()` 完成更新。评估阶段使用 `model.eval()` 与 `torch.inference_mode()`，并保存 `state_dict`、预处理配置、词表或标签表。若本章属于规则、搜索、数据库或治理主题，则 PyTorch 不是强行套用的答案；应保留可解释的 Python 基线，在研究线中再比较神经方法。

形状检查要写在代码里：批次轴、特征轴、序列轴、通道轴不能靠猜。训练曲线至少同时记录训练损失、验证指标和资源成本；只保存最好一次会产生选择偏差。出现 NaN 时先检查输入范围、除零、对数和指数，再检查学习率、梯度范数与混合精度。出现训练好而测试差时先排查泄漏、重复样本、切分方式和分布偏移。

8. 实验设计与结果记录

为本章建立一张实验表。固定问题定义、数据版本、基线、硬件、依赖和随机种子，只改变“现实差距”。每个设置至少运行三次教学模拟；真实研究应根据方差和成本决定更充分的重复次数。结果栏必须标记为“实际测量”“教学模拟”或“文献引用”之一，三者不能混写。

推荐记录字段：实验 ID、日期、假设、唯一改变、数据哈希、代码提交、Python/PyTorch 版本、设备、种子、主要指标、切片指标、时间、内存、失败样例、是否符合预期、下一步。若采用外部结果，记录作者、标题、DOI 或 URL、访问日期、实验环境和原文限制；不要把论文中的一个数字搬到不同数据与硬件上直接比较。

9. 常见失败与排查顺序

275. **问题定义错位。** 指标提高但现实任务没有改善。重新写输入、决策和失败代价。
276. **数据泄漏或重复。** 训练与测试共享样本、时间或主体信息。按真实部署边界重新切分。
277. **表示不一致。** 训练和推理使用不同预处理、词表、单位或类别顺序。把预处理随模型版本化。

278. **只看平均值。** 少数群体、极端场景或长尾失败被平均掩盖。增加切片、区间和最坏情况。

279. **一次改变太多。** 无法归因改进来源。回到单变量实验和消融。

280. **把流畅当正确。** 生成结果自然但证据、逻辑或计算错误。增加引用核对、约束和拒答。

281. **部署条件变化。** 延迟、内存、网络、传感器或用户行为不同。建立监控、降级与回滚。

排查时按“数据→目标→实现→优化→评估→部署→治理”顺序逐层缩小范围。先构造最小可复现失败，再看日志和中间量；不要通过删除失败样本让图表变好。涉及人身、医疗、法律、财务、教育机会或其他高风险决策时，本章练习不能替代专业判断，也不能直接上线。

10. 迁移任务

工程线：把本章最小实现包装成一个可重复运行的命令，加入输入校验、测试、环境文件、日志、模型或规则版本、CPU 资源上限和 README。选择校园图书馆的公开借阅类别作为公开或合成案例，提供一个正常输入、一个边界输入和一个应拒绝的输入。

研究线：选择虚构游戏角色的状态日志，提出一个可证伪问题。复现简单基线，再改变一个机制；至少做一次消融、一次分布变化测试和一次失败类别分析。报告效应大小与不确定性，不只报告最好分数。若结果没有改善，也要解释它排除了什么假设。

11. 三级练习

282. **基础题：** 用自己的话解释“机器学习、仿真到现实与人身安全”，说明它的输入、输出和一个关键假设；再指出生活类比的一个局限。

283. **应用题：** 在公开道路网络与虚构出行任务中设计一个只改变“现实差距”的实验，列出基线、三档设置、指标和失败样例。

284. **挑战题：** 设计一个会让本章方法失效的分布变化或对抗条件，给出检测、拒答、人工复核和回滚方案。

独立答案位于 `content/ai-book/answers/robot-learning-sim2real.md`，网页中默认折叠，建议先完成再核对。

12. 本章能力检查

- 我能在两分钟内说清本章解决的问题与不解决的问题。
- 我能解释核心公式中每个符号的对象、形状和单位。
- 我能运行最小代码，并预测改变一个变量的方向性影响。
- 我能区分教学模拟、实际测量和文献引用。
- 我能给出至少三种失败原因，并按顺序排查。
- 我能说明何时必须停止自动化并交给给人。
- 我能提出一个可证伪研究问题和最低成本基线。

13. 来源与核实

本章来源于下列一手框架、官方文档、开放教材或研究论文的结构化核对；正文为原创解释，不复制原图、习题答案或大段原文。时效内容在每个版本重新核实。

- [S017] Stanford University, 《CS221: Artificial Intelligence》，[访问 stanford-cs221.github.io](https://stanford-cs221.github.io))
- [S044] Open Robotics, 《ROS 2 Documentation》，[访问 docs.ros.org](https://docs.ros.org))
- [S045] Sebastian Thrun, Wolfram Burgard, Dieter Fox, 《Probabilistic Robotics》，[访问 mitpress.mit.edu](https://mitpress.mit.edu))

核实日期：2026-08-06。评审状态：`draft`。只有技术评审、事实核查和专家签字完成后，状态才能按 `draft` → `technical_review` → `fact_checked` → `stable` 前进。

月 18 阶段项目：搭建一个二维机器人安全导航模拟器

项目结论： 实现坐标、传感噪声、定位、路径规划、控制和急停逻辑；所有实验停留在模拟环境。
当前状态为 draft。

交付物

- 问题与边界说明
- 可运行最小实现
- 实验记录与失败分析
- 来源与许可清单
- 风险、隐私与人工闸门
- 复现 README

验收方法

285. 在 CPU 或浏览器主线运行；若使用 GPU，另提供缩小数据冒烟测试。
286. 保存环境、依赖、随机种子、数据许可、测量记录和失败样例。
287. 逐条标记实际测量、教学模拟和文献引用，写清适用边界。
288. 不收集个人信息；高风险输出必须有人审阅、可拒答、可回滚。

独立练习答案

先完成题目、保留自己的推理和错误，再查看参考答案。答案给出最低证据结构，不是唯一正确表述。

第 49 章答案 · 像素、颜色与卷积

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解采样、通道、局部感受野、卷积核和等变性。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“小窗在图像上滑动，重复寻找边缘或纹理；同一规则在不同位置共享。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择合成的植物叶片特征，先用固定规则或简单统计量作为基线。把“卷积核尺寸”设置为 1、3 和 11，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 50 章答案 · CNN、残差网络与迁移学习

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解层级特征、残差连接、预训练和领域差异。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“学会识别形状后再学鸟类，比从随机开始容易；但显微图像和街景差异仍需验证。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择虚构游戏角色的状态日志，先用固定规则或简单统计量作为基线。把“冻结层比例”设置为 0%、70%和 100%，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 51 章答案 · 目标检测、分割与结构化输出

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，区分类别、边界框、像素掩码和实例，理解 IoU 与匹配。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“照片分类回答有什么，检测回答在哪里，分割进一步给出每个像素属于谁。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择公开天文观测的缩小样例，先用固定规则或简单统计量作为基线。把“IoU 阈值”设置为 0、0.5 和 1，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 52 章答案 · 视觉 Transformer、生成视觉与评估

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解图像分块、全局注意力、生成质量评估和数据偏见。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“把图像切成小方块当作视觉词元，让每块与其他块交换信息。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择合成音频波形与环境声标签，先用固定规则或简单统计量作为基线。把“图像块尺寸”设置为 2px、16px 和 32px，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 53 章答案 · 文本、Unicode、分词与词元

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解字符、字节、规范化、词、子词和词表外问题。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“把一段话切成积木；切太大遇到新词，切太小序列变长。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择校园能源使用的匿名汇总数据，先用固定规则或简单统计量作为基线。把“词表大小”设置为 100、8000 和 32000，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 54 章答案 · 词向量、RNN 与 LSTM

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解分布式表示、序列状态、长程依赖和门控记忆。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“读故事时脑中保留摘要，RNN 状态像不断更新的便签；门控决定保留与忘记。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择公开古诗文本与版权已明确的材料，先用固定规则或简单统计量作为基线。把“记忆保留率”设置为 0、0.8 和 1，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 55 章答案 · 注意力与 Transformer

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，从查询、键、值理解内容寻址，掌握多头注意力、位置和因果遮罩。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“查资料时问题是查询，目录线索是键，找到的正文是值。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择虚构机器人在二维网格中的轨迹，先用固定规则或简单统计量作为基线。把“注意力温度”设置为 0.1、1 和 3，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 56 章答案 · NLP 任务、检索、评估与责任

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，覆盖分类、序列标注、生成、检索和事实核查，避免只看流畅度。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“一篇写得顺的答案仍可能引用错页；语言质量和事实证据是两条轴。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择公开科研论文的标题与摘要元数据，先用固定规则或简单统计量作为基线。把“检索候选数”设置为 1 条、5 条和 30 条，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 57 章答案 · 波形、采样与短时傅里叶变换

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解采样率、混叠、频率、相位、窗口和时频图。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“电影用连续照片制造运动，数字音频用离散采样重建波形；采样太慢会混淆高频。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择合成电商目录但不含真实用户行为，先用固定规则或简单统计量作为基线。把“窗口长度”设置为 64 点、512 点和 2048 点，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 58 章答案 · 自动语音识别：声音到文字

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解声学表示、语言信息、CTC 或序列到序列和字错率。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“听写既要辨认声音，也会用句子上下文排除不合理词。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择校园图书馆的公开借阅类别，先用固定规则或简单统计量作为基线。把“束搜索宽度”设置为 1、4 和 20，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 59 章答案 · 语音合成与声码器

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解文本前端、声学模型、声码器、韵律和说话人控制的风险。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“乐谱先描述音高与时长，演奏器再生成真实波形；两阶段可以分别出错。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择不含个人信息的教学模拟天气记录，先用固定规则或简单统计量作为基线。把“采样温度”设置为 0.1、0.8 和 2，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 60 章答案 · 音频理解、音乐与说话人隐私

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，覆盖事件检测、音乐表示、说话人识别与匿名化边界。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“背景声可能泄露地点、家庭成员或健康线索，因此声音不是普通无害输入。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择公开道路网络与虚构出行任务，先用固定规则或简单统计量作为基线。把“隐私预算”设置为 0.1ϵ 、 1ϵ 和 10ϵ ，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 61 章答案 · 生成建模与变分自编码器

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，区分显式、隐式生成，理解潜变量、重参数化和证据下界。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“把复杂图像压进一张连续地图，再从地图附近采样重建新图案。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择合成的植物叶片特征，先用固定规则或简单统计量作为基线。把“潜变量维度”设置为 2、16 和 128，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 62 章答案 · 生成对抗网络

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解生成器与判别器的博弈、模式崩溃、训练不稳和评估。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“伪造者和鉴定师相互进步，但如果伪造者只会一种样式，就出现模式崩溃。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择虚构游戏角色的状态日志，先用固定规则或简单统计量作为基线。把“判别器步数”设置为 1 步、1 步和 10 步，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 63 章答案 · 扩散模型与分数匹配

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解加噪、去噪、分数函数、采样步数和条件引导。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“先逐步把照片打散成雪花，再学习每一步怎样去掉一点噪声。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择公开天文观测的缩小样例，先用固定规则或简单统计量作为基线。把“去噪步数”设置为 5 步、50 步和 1000 步，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 64 章答案 · 流模型、能量模型与生成评估

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解可逆变换、连续流、能量函数和质量/多样性/记忆风险。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“把简单分布像橡皮泥一样连续变形成复杂分布，同时追踪体积变化。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择合成音频波形与环境声标签，先用固定规则或简单统计量作为基线。把“引导强度”设置为 0、7.5 和 20，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 65 章答案 · MDP、回报与贝尔曼方程

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解状态、动作、转移、奖励、折扣和马尔可夫假设。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“走迷宫时每步位置是状态，选择方向是动作，终点奖励与撞墙代价共同塑造策略。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择校园能源使用的匿名汇总数据，先用固定规则或简单统计量作为基线。把“折扣因子”设置为 0γ 、 0.95γ 和 1γ ，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 66 章答案 · 价值学习、Q-learning 与 DQN

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，从时序差分更新到经验回放、目标网络和过估计问题。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“学生把新一次结果与原先预期比较，用差值更新对动作价值的判断。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择公开古诗文本与版权已明确的材料，先用固定规则或简单统计量作为基线。把“探索率”设置为 0ϵ 、 0.2ϵ 和 1ϵ ，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 67 章答案 · 策略梯度、Actor-Critic 与 PPO

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，直接优化策略概率，用价值基线降方差，理解裁剪目标。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“演员选择动作，评论员估计表现；两者互相纠正但也可能共同偏离。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择虚构机器人在二维网格中的轨迹，先用固定规则或简单统计量作为基线。把“裁剪范围”设置为 0.05、0.2 和 0.5，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 68 章答案 · 模型式、离线、多智能体与安全 RL

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解环境模型、分布外动作、信用分配、约束和安全探索。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“只看旧棋谱学策略时，没出现过的走法价值很难可靠估计。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择公开科研论文的标题与摘要元数据，先用固定规则或简单统计量作为基线。把“分布偏移”设置为 0%、25%和 100%，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 69 章答案 · 坐标、运动学与动力学

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解坐标系、位姿、关节、正逆运动学、速度与力。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“机械臂各关节像手臂骨骼；末端位置由所有关节角度共同决定。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择合成电商目录但不含真实用户行为，先用固定规则或简单统计量作为基线。把“关节角度”设置为 -180° 、 0° 和 180° ，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 70 章答案 · 传感、定位、地图与 SLAM

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，融合带噪观测，在未知环境同时估计位姿与地图。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“在黑屋里一边摸墙一边画地图，你的位置估计和地图会互相影响。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择校园图书馆的公开借阅类别，先用固定规则或简单统计量作为基线。把“传感噪声”设置为 0%、10%和 100%，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 71 章答案 · 运动规划与反馈控制

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，区分几何路径、时间轨迹和反馈控制，理解 PID 与模型预测控制。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“导航先画路线，驾驶还要持续根据偏差修方向；计划和控制不能混为一谈。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择不含个人信息的教学模拟天气记录，先用固定规则或简单统计量作为基线。把“比例增益”设置为 0Kp、1Kp 和 10Kp，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

第 72 章答案 · 机器人学习、仿真到现实与人身安全

答案用于自检，不是唯一表述。先保留自己的推理，再比较遗漏。

基础题参考

合格答案应包含三部分：第一，理解模仿学习、强化学习、域随机化、现实差距和物理安全闸门。；第二，输入、内部机制和输出之间的关系；第三，至少一个适用假设。生活类比“飞行模拟器能练习，但真实风、传感故障和人员靠近带来额外风险。”能提供直觉，但它省略了数学约束、数据偏差和部署风险，因此不能作为实验证据。若只写概念定义、没有边界或反例，答案仍不完整。

应用题参考

选择公开道路网络与虚构出行任务，先用固定规则或简单统计量作为基线。把“现实差距”设置为 0%、20%和 100%，其余条件保持一致。记录主要指标、资源成本、至少一个切片和失败样例。页面结果必须写“教学模拟”；如果自己运行真实代码，则保存环境、数据版本、种子和测量记录后才能写“实际测量”。

挑战题参考

可以主动改变输入分布、加入噪声、制造缺失、交换标签含义或改变部署资源。检测层使用输入校验、漂移或分布外分数；决策层设置置信阈值和拒答；流程层对高风险输出要求人工复核；运维层保留上一版本、变更记录和回滚触发条件。关键不是列工具名，而是说明每道控制对应哪个失败路径、由谁负责、怎样验证控制有效。

自评量规

- 0 分：只复述名词。

- 1 分：说明了机制，但没有实验或边界。
- 2 分：有基线、单变量、指标和失败分析。
- 3 分：进一步包含不确定性、迁移、人工闸门和可复现记录。

本卷来源台账

本卷共引用 23 条来源。正文为原创解释；不复制受版权保护的图表、习题答案或大段原文。访问日期均为当前 Beta 版核实记录。

[S017] CS221: Artificial Intelligence

项目	内容
作者/机构	Stanford University
来源等级	大学课程一手资料
发布日期	持续更新
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 stanford-cs221.github.io

[S026] CS231n: Deep Learning for Computer Vision

项目	内容
作者/机构	Stanford University
来源等级	大学课程一手资料
发布日期	2026

项目	内容
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 cs231n.stanford.edu

[S027] Deep Residual Learning for Image Recognition

项目	内容
作者/机构	Kaiming He et al.
来源等级	同行评审论文预印本
发布日期	2015
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

[S028] An Image is Worth 16x16 Words

项目	内容
作者/机构	Alexey Dosovitskiy et al.

项目	内容
来源等级	同行评审论文预印本
发布日期	2020
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

[S029] CS224N: Natural Language Processing with Deep Learning

项目	内容
作者/机构	Stanford University
来源等级	大学课程一手资料
发布日期	2026
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 web.stanford.edu

[S030] Attention Is All You Need

项目	内容
作者/机构	Ashish Vaswani et al.
来源等级	同行评审论文预印本
发布日期	2017
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

[S031] BERT: Pre-training of Deep Bidirectional Transformers

项目	内容
作者/机构	Jacob Devlin et al.
来源等级	同行评审论文预印本
发布日期	2018
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名

项目	内容
	名
DOI/URL	访问 arxiv.org

[S032] TorchAudio Documentation

项目	内容
作者/机构	PyTorch
来源等级	官方文档
发布日期	持续更新
访问日期	2026-08-06
许可	BSD-2-Clause
DOI/URL	访问 docs.pytorch.org

[S033] Deep Speech

项目	内容
作者/机构	Awni Hannun et al.
来源等级	研究论文预印本

项目	内容
发布日期	2014
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

[S034] WaveNet

项目	内容
作者/机构	Aaron van den Oord et al.
来源等级	研究论文预印本
发布日期	2016
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

[S035] Auto-Encoding Variational Bayes

项目	内容
作者/机构	Diederik P. Kingma, Max Welling
来源等级	同行评审论文预印本
发布日期	2013
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

[S036] Generative Adversarial Nets

项目	内容
作者/机构	Ian Goodfellow et al.
来源等级	同行评审论文预印本
发布日期	2014
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名

项目	内容
	名
DOI/URL	访问 arxiv.org

[S037] Denoising Diffusion Probabilistic Models

项目	内容
作者/机构	Jonathan Ho et al.
来源等级	同行评审论文预印本
发布日期	2020
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

[S038] Score-Based Generative Modeling through Stochastic Differential Equations

项目	内容
作者/机构	Yang Song et al.

项目	内容
来源等级	同行评审论文预印本
发布日期	2020
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

[S039] Flow Matching for Generative Modeling

项目	内容
作者/机构	Yaron Lipman et al.
来源等级	同行评审论文预印本
发布日期	2022
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

[S040] Reinforcement Learning: An Introduction

项目	内容
作者/机构	Richard Sutton, Andrew Barto
来源等级	作者开放教材
发布日期	2018
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 incompleteideas.net

[S041] CS 285: Deep Reinforcement Learning

项目	内容
作者/机构	UC Berkeley
来源等级	大学课程一手资料
发布日期	持续更新
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 rail.eecs.berkeley.edu

[S042] Human-level control through deep reinforcement learning

项目	内容
作者/机构	Volodymyr Mnih et al.
来源等级	同行评审论文
发布日期	2015
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 doi.org

[S043] Proximal Policy Optimization Algorithms

项目	内容
作者/机构	John Schulman et al.
来源等级	研究论文预印本
发布日期	2017
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名

项目	内容
	名
DOI/URL	访问 arxiv.org

[S044] ROS 2 Documentation

项目	内容
作者/机构	Open Robotics
来源等级	官方文档
发布日期	持续更新
访问日期	2026-08-06
许可	Apache-2.0
DOI/URL	访问 docs.ros.org

[S045] Probabilistic Robotics

项目	内容
作者/机构	Sebastian Thrun, Wolfram Burgard, Dieter Fox
来源等级	经典教材出版信息

项目	内容
发布日期	2005
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 mitpress.mit.edu

[S055] Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks

项目	内容
作者/机构	Patrick Lewis et al.
来源等级	同行评审论文预印本
发布日期	2020
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

[S071] Model Cards for Model Reporting

项目	内容
----	----

项目	内容
作者/机构	Margaret Mitchell et al.
来源等级	同行评审论文预印本
发布日期	2018
访问日期	2026-08-06
许可	以来源页许可为准；本书仅作原创解释、短引用与明确署名
DOI/URL	访问 arxiv.org

全书术语表

共 81 个核心术语。定义用于建立共同语言，不能替代章节中的数学、实验和边界分析。

术语	英文	小白解释
人工智能	Artificial Intelligence	让机器执行通常需要感知、推理、学习、规划或生成等能力的研究与工程领域。
算法	Algorithm	把输入转换为输出的一组明确步骤；算法本身不等于训练后的模型。
模型	Model	从数据或规则中得到、用于预测或决策的数学结构及其参数。
参数	Parameter	训练过程中被优化的数值，例如神经网络权重。
超参数	Hyperparameter	由开发者或搜索过程设定、不是直接从单次梯度更新学得s的配置。
数据集	Dataset	带有明确来源、字段、许可和用途的一组样本。

术语	英文	小白解释
特征	Feature	模型使用的输入表示。
标签	Label	监督学习中希望模型预测的目标值。
训练	Training	用目标函数和优化方法调整模型参数的过程。
推理	Inference	用已经得到的模型对新输入计算输出。
损失函数	Loss function	把预测与目标之间的差异变成可优化数值的函数。
目标函数	Objective	训练或决策希望最大化或最小化的量，可能包含多个损失和约束。
梯度	Gradient	函数对多个变量的一阶变化率组成的向量。
泛化	Generalization	模型在未参与训练、但与目标场景相关的数据上保持能力。
过拟合	Overfitting	模型过度适应训练数据细节，导致新数据表现下降。

术语	英文	小白解释
欠拟合	Underfitting	模型或训练不足以捕捉任务中的重要结构。
正则化	Regularization	通过惩罚、噪声或结构限制降低过拟合风险的方法。
基线	Baseline	用于判断新方法是否真正改进的简单或既有方法。
消融实验	Ablation	移除或替换系统一部分，观察它对结果的贡献。
随机种子	Random seed	初始化伪随机数生成器的值；固定种子不是完整可复现性的替代品。
张量	Tensor	带有一个或多个轴的数值数组。
嵌入	Embedding	把离散对象映射到连续向量空间的表示。
注意力	Attention	根据查询与键的匹配程度加权汇总值的机制。
Transformer	—	以注意力、前馈层、残差和归一化为核心的序列模型架构。

术语	英文	小白解释
词元	Token	文本经过词元器切分后的基本单位，可是字符、子词或其他片段。
上下文窗口	Context window	模型一次计算中能够直接处理的词元范围。
基础模型	Foundation model	在广泛数据上训练、可适配多种下游任务的大规模模型。
语言模型	Language model	为词元序列分配概率或预测后续词元的模型。
检索增强生成	RAG	在生成前检索外部资料，并把证据提供给生成模型的系统模式。
Agent	—	围绕目标执行观察、计划、工具调用、验证和停止循环的系统。
提示注入	Prompt injection	不可信输入试图改变模型或 Agent 原定指令和权限的攻击。
强化学习	Reinforcement learning	智能体通过与环境交互、基于

术语	英文	小白解释
		奖励学习策略的方法。
策略	Policy	在给定状态下选择动作的规则或概率分布。
价值函数	Value function	从状态或状态动作对出发的预期累计回报。
马尔可夫决策过程	MDP	用状态、动作、转移、奖励和折扣描述序列决策的形式框架。
卷积	Convolution	用共享局部核在输入位置上滑动计算的运算。
计算机视觉	Computer vision	让机器从图像或视频中提取、生成和使用信息的领域。
自然语言处理	NLP	让计算机处理、理解、检索或生成人类语言的领域。
自动语音识别	ASR	把语音波形转换为文字或其他符号序列。
扩散模型	Diffusion model	通过学习逐步去噪过程生成样本的一类模型。

术语	英文	小白解释
生成对抗网络	GAN	通过生成器与判别器对抗训练学习生成分布的架构。
图神经网络	GNN	在图结构上通过邻域聚合或消息传递学习表示的模型。
校准	Calibration	预测概率与事件长期发生频率之间的一致程度。
分布偏移	Distribution shift	训练、评估与部署数据分布不一致的现象。
分布外	OOD	与训练或预期部署分布明显不同的输入。
因果推断	Causal inference	在明确假设下估计干预对结果影响的方法。
公平性	Fairness	围绕不同群体或个体的机会、错误、待遇和影响制定并审查的规范目标。
鲁棒性	Robustness	系统面对扰动、噪声、故障或环境变化仍保持可接受行为的能力。
可解释性	Explainability	为模型行为提供可理解说明的

术语	英文	小白解释
		方法和性质；解释清楚不等于预测正确。
差分隐私	Differential privacy	通过限制单条记录对输出分布的影响提供可量化隐私保证的框架。
联邦学习	Federated learning	在数据留在多个设备或组织的情况下协同训练的范式。
模型卡	Model card	记录模型用途、评估、限制和 risk 的结构化文档。
数据表	Datasheet	记录数据来源、构建、用途、限制和维护方式的结构化文档。
MLOps	—	管理机器学习数据、训练、部署、监控、版本和事故响应的工程实践。
延迟	Latency	一次请求从进入到完成所需的时间。
吞吐	Throughput	单位时间内系统能处理的请求或词元数量。

术语	英文	小白解释
量化	Quantization	用较低精度数值表示权重或激活以降低资源成本的方法。
蒸馏	Distillation	让较小模型学习较大模型输出或内部结构的方法。
并行训练	Distributed training	把训练计算、数据或参数分布到多个设备或进程。
检查点	Checkpoint	保存训练状态以便恢复、评估或部署的版本化工件。
可复现	Reproducible	他人依据充分工件和说明能够得到相容结果的性质。
同行评审	Peer review	由相关领域同行对方法、证据和表述进行独立审查。
置信区间	Confidence interval	按指定重复抽样程序构造、具有长期覆盖率解释的区间。
p 值	p-value	在零假设及检验假设成立时，观察到至少同样极端统计量的概率。
效应量	Effect size	差异或关联实际大小的度量。

术语	英文	小白解释
熵	Entropy	概率分布不确定性的度量。
交叉熵	Cross entropy	用一个分布编码另一个分布时的平均信息量，也是常见分类损失。
KL 散度	KL divergence	衡量一个概率分布相对另一个分布差异的非对称量。
贝叶斯更新	Bayesian update	用似然把先验信念更新为后验信念。
知识图谱	Knowledge graph	用实体、关系和属性构成的结构化知识网络。
本体	Ontology	对领域概念、关系和约束的显式规范。
搜索启发式	Heuristic	估计距离或代价、用于决定优先探索方向的函数。
约束满足	CSP	为变量选择值，使所有约束同时满足的问题。
SLAM	—	机器人同时定位并建立环境地图的问题。

术语	英文	小白解释
控制	Control	根据目标与反馈选择输入，使动态系统按期望演化。
仿真到现实	Sim-to-real	把在仿真中得到的方法迁移到真实系统的过程及差距问题。
世界模型	World model	学习环境状态和动作如何随时间演化的内部模型。
多模态	Multimodal	联合处理文本、图像、音频、视频或动作等多种信息形式。
AI for Science	—	使用 AI 辅助科学建模、模拟、实验设计、分析和发现的方向。
人机协同	Human-in-the-loop	在系统关键环节保留明确人工检查、判断或控制权的设计。
风险	Risk	事件发生可能性与后果的组合，必须结合具体情境评估。

版权、版本与勘误

2026.08 Beta · 第三卷：主要 AI 分支 · 评审状态 draft。

Copyright © 2026 NEWVAR LAB. All rights reserved.

全部原创正文、实验定义和代码保留全部版权。第三方名称、论文与链接仅作明确署名的教学引用，其权利归原权利人。

本书仍处于 Beta：可能存在表达、事实、代码或排版问题。请通过 NEWVAR 版本页查看核实日期、评审状态与更正记录。

任何时效性结论都应在使用前回到一手来源重新核实；医疗、法律、财务、教育机会和安全关键场景必须由合格专业人员判断。

学习网站：[访问 newvarlab.com](https://newvarlab.com)）。