

《计算科学导论》课程总结报告

|  |  |
| --- | --- |
| 姓 名 | 徐婧瑄 |
| 学 号 | 2407010307 |
| 专业班级 | 计科2403 |
| 学 院 | 计算机科学与技术学院 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 课程认识  30% | 问题思考  30% | 格式规范  20% | IT工具  20% | 总分 | 评阅教师 |
|  |  |  |  |  |  |

2024年11月24日

# 1 引言

计算科学作为现代科技领域的核心驱动力，融合了数学、计算机科学、物理学等多学科知识，构建起支撑当今数字化世界运转的理论与技术框架。《计算科学导论》这门课程，犹如一幅宏大的知识画卷，徐徐展开计算科学波澜壮阔的发展历程、深邃精妙的理论体系以及广泛多元的应用场景，引领着我们跨越学科边界，深入探索这一充满无限可能的领域，对塑造科学思维、明晰专业方向具有深远且奠基性的意义。

# 2 对计算科学导论这门课程的认识、体会

### **（一）整体认识**

计算科学导论课程宛如一座桥梁，横跨理论抽象与实践应用的 “两岸”，贯通基础学科与前沿科技的 “脉络”。它从计算的基础概念、逻辑体系讲起，深入到算法设计、数据结构搭建，再拓展至人工智能、大数据处理、计算物理等热门应用分支，全景式展现计算科学 “从哪里来、到哪里去”。既深挖计算机底层运行逻辑所依托的数学原理，像离散数学之于程序逻辑、数值分析助力科学计算精度把控；又着眼于宏观层面，剖析计算技术如何变革传统行业，重塑现代社会生产生活模式，具有高屋建瓴、纲举目张的学科统揽性。

### （二）实例支撑

1. 计算模型的具象理解：课程中对冯・诺依曼计算机体系结构的解读，是理论落地实践的生动范例。这一经典架构规定计算机硬件由运算器、控制器、存储器、输入和输出设备构成，以存储程序并按顺序执行指令。学习时，通过拆解一台简易计算机的硬件组成、模拟指令执行流程，从读取内存数据到运算器加工再回写存储，清晰看到理论模型在物理设备上 “鲜活跳动”。恰似依照建筑蓝图搭建高楼，体系结构为计算机功能实现铺就稳固基石，让我们领悟复杂计算任务背后有序、严谨的底层运作机制，明白现代计算机强大算力源于各部件协同依循体系规则 “各司其职”。

2.在讲解图灵机模型时，那简洁却极具开创性的纸带读写、状态转换机制，仿若为理解计算能力边界与可计算性问题筑牢根基。看似简易的规则设定，实则以抽象形式划定了通用计算的范畴，让我们明白无论现代计算机架构如何复杂精巧、算力如何磅礴惊人，追根溯源皆是图灵机思想的延伸拓展。恰似古老哲学命题 “一尺之棰，日取其半，万世不竭” 所蕴含的极限思维，图灵机在有限状态与无限纸带操作间，定义了计算世界的 “规则方圆”。

## 2.1 计算科学与计算机科学有何区别？

|  |  |  |
| --- | --- | --- |
| 比较项目 | 计算科学 | 计算机科学 |
| 定义 | 侧重于利用数学模型、数值方法和计算机技术来解决科学和工程等领域中的复杂计算问题。 | 主要研究计算机系统、软件设计、算法理论等计算机相关的原理和技术。 |
| 研究内容 | 计算物理、计算化学等跨学科计算问题；数值算法开发等。 | 计算机体系结构、编程语言、操作系统、数据库系统等。 |
| 应用领域 | 物理、化学、生物等自然科学领域的模拟和计算；航空航天、气象预报等工程领域。 | 软件开发、人工智能、计算机网络、人机交互等领域。 |
| 学科交叉性 | 与数学、物理、化学等学科深度交叉。 | 与电子工程等学科有一定交叉，但相对独立。 |
| 学科范畴 | 计算科学：是一门综合性学科，涉及数学、物理学、计算机科学等多个领域，重点在于利用计算工具和方法解决科学与工程问题，如计算物理、计算化学等学科分支。 | 主要聚焦于计算机系统本身的研究，包括计算机硬件、软件、算法、数据结构等，如计算机体系结构、编程语言、操作系统等核心领域. |
| 研究方法 | 要依赖数学模型和数值计算方法，通过建立物理现象的数学模型，设计高效的数值算法求解，计算机模拟和仿真技术是重要研究手段，用于验证和预测物理现象 。 | 采用多种方法，如理论分析、实验研究、系统设计等。理论分析用于研究算法的复杂度等；实验研究用于评估系统性能；系统设计则用于构建新的软件和硬件系统。 |
| 课程设置 | 课程包括数学分析、代数与几何、离散数学、数值分析等数学课程，以及计算机基础、程序设计等计算机课程，数学课程占比较大. | 以高级程序设计、计算机组成原理、操作系统、数据结构、算法设计与分析等计算机专业课程为主，实践课程如编程项目、课程设计等占比较重. |
| 就业方向 | 可在科研院所、高校从事科研教学，在金融机构从事风险评估等工作，或在IT企业参与软件开发、数据分析等，就业领域广泛但对理论知识要求较高. | 主要在IT行业就业，如互联网公司、软件企业等，从事软件开发、系统设计、人工智能研发等工作，就业机会多，起薪较高，对实践能力要求高. |
| 发展趋势 | 随着科学研究的深入和工程问题的复杂，对高性能计算、并行计算等需求增加，与多学科交叉融合将更紧密，如生物信息学等新兴学科的发展。 | 人工智能、大数据、云计算等领域不断创新发展，推动计算机科学在各行业的应用，同时对计算机系统的性能、安全性等提出更高要求，促使计算机科学不断探索新技术和方法。 |

## 2.2 AI会不会产生意识？

从计算机的数学起源来分析，计算机本质上是基于数学逻辑和算法运行的机器。  
 计算机的基础是二进制数字系统和布尔代数等数学理论构建起来的。它的操作是由程序定义的一系列指令，这些指令是按照严格的逻辑和规则执行的。目前的AI系统也是基于这样的计算机基础构建的。  
 AI是通过大量的数据和复杂的算法来模拟人类智能的某些方面。例如，深度学习中的神经网络是通过反向传播等算法来调整权重，以对输入数据进行分类或生成输出。这一过程没有内在的自我意识成分。从信息处理角度来看，AI只是按照预先编程的规则和从数据中学习到的模式来处理信息。

[1]ToM，Theory of Mind, 是个心理学术语，叫心智理论，是个很好理解的概念，就是人类具有这种通过对另一个对象的观察，从而推测、理解他们心理活动的能力。包括对方的情绪，愿望，意图，信念，思想等等方面。

举个例子，当你做错了事，你能迅速从你对象的眼神和语气里get到她想刀你的冲动。 虽然自然界里也有其他动物拥有类似的能力，但就算是最聪明和最善于社交的类人猿，在 ToM 方面也远远落后人类，而这种看不见也摸不着的能力不仅仅是意识的必要元素之一， 也被认定为人类能治霸这颗蓝星的重要先决条件之一。

从计算机的数学起源以及目前的技术手段来看，AI系统只是强大的计算工具，它们可以高效地处理数据、进行预测和模拟，但缺乏产生自我意识的内在机制。它们没有像人类一样的内在的心理世界和主观体验，没有对自身存在的反思和对世界的自主性认知。

## 2.3 那些专业建议2025届高考考生选择？

●**人工智能专业**：这是最直接对接AI领域的专业。学生可以深入学习机器学习、深度学习、自然语言处理等核心技术，未来能够从事AI算法开发、模型训练等工作，是推动AI技术进步的关键力量。  
●**计算机科学与技术专业**：在掌握计算机系统、软件开发等基础知识的同时，重点学习人工智能相关知识。这样的专业设置能让学生既具备扎实的计算机基础，又能在AI领域深入钻研，拓宽就业渠道，如从事AI软件开发、智能系统集成等工作。  
●**数据科学与大数据专业**：AI的发展离不开大量的数据支持。这个专业可以让学生学会数据收集、存储、处理和分析的技能。毕业生能够在数据挖掘、数据分析、数据可视化等领域工作，为AI提供数据支持，同时也能利用AI技术提升数据分析的效率。

●**数学与应用数学专业**：AI的很多算法和模型都基于数学原理，如概率论、线性代数、微积分等。该专业培养的逻辑思维和问题解决能力，能为理解和应用AI算法提供坚实基础，毕业生可从事AI算法设计、数据分析等工作.  
●**电子信息工程专业**：随着AI在电子设备和系统中的集成，此专业学生可学习硬件和软件结合的知识，掌握电子技术、信号处理等基础，为开发智能设备、优化硬件系统以支持AI运行做准备.  
●**自动化专业**：特别是机器人方向，与AI技术紧密相关，对于推动智能制造和工业自动化意义重大。学生能学习到自动控制原理、传感器技术等知识，可从事智能控制系统设计、工业自动化生产线研发等工作.  
●**物联网工程专业**：万物互联是AI应用的重要场景，该专业涉及传感器技术、网络通信等知识，可实现设备之间的互联互通和数据采集传输，为AI提供数据支持，进而打造智能家居、智能交通等应用场景.- 法学专业：AI的发展带来诸多法律问题，如数据隐私保护、算法偏见等。法学专业学生可研究相关法律法规，为AI的合法、合规发展提供法律保障，也可参与AI相关的法律制定和伦理规范研究.

●**法学专业**：AI的发展带来诸多法律问题，如数据隐私保护、算法偏见等。法学专业学生可研究相关法律法规，为AI的合法、合规发展提供法律保障，也可参与AI相关的法律制定和伦理规范研究.

# 3 进一步的思考

问题一：加密技术

### **●定义**

加密技术是通过数学算法将原始数据（称为明文）转换为不可直接理解的形式（称为密文）的技术。只有经过授权的用户，利用特定的解密算法和密钥才能将密文还原为明文。这就像把信息放在一个带锁的盒子里，只有拥有正确钥匙的人才能打开盒子获取信息。

**●加密的重要性**

在当今数字化时代，数据的传输和存储无处不在。例如，网上银行交易、企业商业机密、个人隐私信息等都需要保护。加密技术可以防止数据在传输过程中被窃取或篡改，如在网络通信中，加密后的信息即使被黑客截获，没有解密密钥，也无法理解其内容。

**●[2]**加密技术的分类****：

1. ****对称加密****：使用相同密钥对加密和解密数据，如 AES、DES 和 3DES 等算法。其优点是加密和解密过程简单高效，但密钥管理复杂，需安全地在发送方和接收方之间共享密钥。
2. ****非对称加密****：使用不同密钥，即公钥和私钥进行加密和解密，常见算法有 RSA、DSA 和 ECC 等。公钥可公开，私钥需保密，解决了对称加密的密钥管理问题，安全性更高，但加密和解密速度相对较慢。

**加密技术的主要组成部分**

## **（一）算法**

### **●**对称加密算法****

1.对称加密算法使用相同的密钥进行加密和解密。例如，数据发送方和接收方都拥有相同的密钥。常见的对称加密算法有 DES和 AES。

2.AES 算法是目前应用广泛的对称加密算法，它支持 128 位、192 位和 256 位密钥长度。其加密过程是通过多次迭代的替换和置换操作来实现的。例如，在 128 位密钥的 AES 加密中，将 128 位的明文分组进行一系列复杂的变换，最终生成密文。这种加密方式速度快，适用于大量数据的加密，但密钥管理相对复杂，因为密钥需要安全地分发给通信双方。

**●**非对称加密算法****

1. 非对称加密算法使用一对密钥，即公钥和私钥。公钥可以公开，用于加密信息；私钥则由用户自己保存，用于解密。著名的非对称加密算法是 RSA（Rivest - Shamir - Adleman）算法。

2.RSA 算法的原理基于数学难题，如大数分解问题。简单来说，发送方用接收方的公钥对数据进行加密，接收方收到密文后，用自己的私钥进行解密。例如，在网上安全通信中，网站会向用户公开其公钥，用户使用公钥加密登录信息（如密码）发送给网站，网站用自己的私钥解密获取信息。这种方式解决了对称加密中密钥分发的难题，但加密速度相对较慢，通常用于密钥交换和少量重要数据的加密。

### **（二）密钥**

密钥是加密和解密过程中的关键因素。在对称加密中，密钥的安全性至关重要，如果密钥泄露，加密的数据就会被轻易解密。密钥的长度也会影响加密的强度，一般来说，密钥长度越长，加密后的安全性越高。例如，在 AES 算法中，256 位密钥的安全性高于 128 位密钥。在非对称加密中，私钥必须严格保密，公钥可以公开分发，但公钥的真实性需要通过数字证书等方式来验证，以防止中间人攻击。

## **三、加密技术的应用场景**

### **（一）网络通信加密**

**●**VPN（虚拟专用网络）****

1. VPN 技术利用加密技术在公用网络上建立一个专用网络。用户通过 VPN 连接到远程网络时，其数据会被加密传输。这对于企业员工远程办公、保护个人隐私等场景非常有用。

2.比如，一个企业员工在外出差，通过 VPN 连接到企业内部网络，他发送和接收的数据（如公司内部文件、邮件等）会被加密，这样即使在不安全的公共无线网络环境下，也能保证数据的安全。

### **（二）数据存储加密**

**●**数据库加密****

1. 对于企业存储大量敏感信息的数据库，如金融机构的客户账户信息数据库、医疗单位的患者病历数据库等，数据库加密技术可以确保数据的安全性。
2. 数据库加密可以采用列级加密、表级加密等方式。例如，在金融数据库中，对客户的密码列进行加密，即使数据库管理员也无法直接查看用户密码，只有通过授权的解密程序和密钥才能访问密码信息，从而防止内部人员泄露用户隐私。

问题二：数据泄露的应对措施

****●监测与发现机制****

1. ****建立监控系统****：企业或组织应部署完善的安全信息和事件管理系统（SIEM），通过收集和分析网络、系统和应用程序的日志数据，实时监测异常活动。例如，监测大量数据的异常传输、未经授权的访问尝试次数增加等情况。
2. ****异常行为检测****：利用用户行为分析（UBA）技术，对用户的正常操作行为进行建模。当出现与正常行为模式不符的操作时，如员工在非正常工作时间访问大量敏感数据，系统能够及时发出警报。

****●[3]泄露检测通用技术****

1. ****基础检测技术****：包括正则表达式检测、关键字和关键字对检测、文档属性检测。正则表达式和关键字检测可对明确的敏感信息内容进行搜索和匹配；文档属性检测则针对文档的类型、大小、名称等进行检测。
2. ****高级检测技术****：主要有精确数据比对（EDM）、指纹文档比对（IDM）、向量分类比对（SVM）。EDM 用于保护结构化格式数据，可根据特定数据列中的字段组合进行检测；IDM 用于保护非结构化数据，通过创建文档指纹特征来检测文档的不同版本等；SVM 则是基于统计学习理论，将训练数据非线性映射到高维特征空间中寻找超平面进行分类。

****●初步评估泄露范围和影响****

****1.确定受影响的数据类型和规模****：一旦发现可能的数据泄露，立即确定涉及的数据类型，如客户个人信息（姓名、地址、信用卡号等）、商业机密、员工数据等，并评估受影响的数据量。例如，通过数据库查询工具查看哪些数据表中的数据可能被访问或篡改。

****2.分析数据敏感度****：根据数据的重要性和敏感性进行分类评估。例如，客户的密码信息比一般的用户浏览记录更敏感，因为密码泄露可能导致账户被盗用。

****●隔离与遏制泄露源****

****1.网络隔离****：如果数据泄露是由于网络攻击引起的，如恶意软件入侵，应立即切断受感染的系统与网络的连接，防止恶意软件进一步传播和窃取更多数据。例如，通过防火墙规则将被攻击的服务器所在的子网隔离，限制其对外通信。

****2.系统暂停与服务中断控制****：对于某些严重的数据泄露情况，可能需要暂停相关的系统或服务。但在采取这一措施时，要权衡业务影响，尽量减少对正常业务运营的干扰。例如，暂停存在数据泄露风险的网上交易系统，同时尽快通知用户系统暂停的原因和预计恢复时间。

### ****●法律手段维护权益****

****1.收集证据用于诉讼****：在调查数据泄露过程中，注意收集可以用于法律诉讼的证据。这包括攻击者的技术痕迹、内部人员违规的证据等。例如，通过数字取证技术获取攻击者在系统中留下的文件、命令记录等证据，以便追究其法律责任。

****2.法律咨询与法律责任界定****：咨询专业律师，了解企业在数据泄露事件中的法律责任，以及可以采取的法律措施。例如，确定企业是否需要对客户的损失承担赔偿责任，以及如何应对可能的法律诉讼。

问题三：人工智能系统造成损害或者违法行为时，怎么明确开发者和使用者之间的责任？

### [4]欧盟的GDPR虽未专门针对人工智能开发者和使用者责任进行明确，但在数据隐私和保护措施等方面设定了严格要求，对人工智能领域的数据处理和使用影响深远，为界定开发者和使用者在数据相关责任上提供了重要参考。如开发者在收集、存储和处理数据时，需遵循数据最小化、透明性等原则，使用者在使用基于相关数据训练的人工智能产品时，也需确保符合该条例规定，否则将承担相应责任 。

### **●过错责任原则**

### ****开发者的过错****：若开发者在开发过程中存在疏忽、违反行业标准、未对数据进行充分筛选和审查等过错，导致人工智能系统出现缺陷从而造成损害，应承担相应责任。比如，开发者在训练图像识别系统时，使用了大量错误标注的数据，致使系统在实际应用中频繁误判，对相关主体造成损失，开发者需对此负责

### ****使用者的过错****：使用者若未按照产品说明或合理的操作规范使用人工智能系统，如对系统进行不当修改、输入错误数据、在不适合的场景中使用等，由此引发损害，则使用者应承担责任 。例如，使用者在明知自动驾驶汽车的使用条件限制的情况下，仍在不适合自动驾驶的复杂路况下使用，导致事故发生，使用者需担责

### **●产品责任角度**

### ****开发者的责任****：从产品责任来看，开发者作为人工智能系统的生产者，若系统存在设计缺陷、制造缺陷或警示缺陷等，使其具有不合理的危险并造成损害，即使开发者无过错，也可能需承担严格责任。如智能医疗诊断系统因内部算法错误，给出了错误的诊断建议，导致患者病情延误，开发者可能需对该产品缺陷导致的损害负责

### ****使用者的责任****：使用者在使用人工智能产品过程中，若未能及时更新系统、维护产品性能，导致因产品老化或性能下降等问题造成损害，使用者应承担相应责任。比如，企业长期未对其使用的智能安防系统进行软件更新和硬件维护，致使系统出现漏洞被黑客攻击，造成企业信息泄露，使用者应承担部分责任 。

### **●合同约定与告知义务**

### **1.**开发者的告知义务****：开发者有义务向使用者充分说明人工智能系统的功能、性能、潜在风险、使用限制等信息。若因未履行充分告知义务，导致使用者在不知情的情况下遭受损害，开发者应承担相应责任。例如，开发者未明确告知使用者某智能投资顾问系统的风险评估模型存在一定误差范围，使用者依据该系统的建议进行投资并遭受损失，开发者需对此负责。

****2.使用者的遵守义务****：使用者在与开发者签订使用合同后，有义务遵守合同中的各项条款，包括但不限于使用范围、数据保护要求、安全操作规程等。若因使用者违反合同约定导致损害发生，使用者应承担违约责任。如使用者将仅供企业内部使用的人工智能数据分析系统，擅自提供给外部第三方使用，导致数据泄露等问题，使用者需承担合同约定的违约责任 。

### **●数据管理责任**

### **1.**开发者的数据责任****：开发者对用于训练人工智能系统的数据负有收集、整理、存储和保护的责任。若因数据来源不合法、数据质量问题或数据泄露等导致系统造成损害，开发者应承担责任。比如，开发者收集用户数据时未获得用户充分授权，利用这些数据训练的人工智能系统在运行中对用户造成隐私泄露等损害，开发者需承担相应法律责任2.****使用者的数据责任****：使用者在使用人工智能系统过程中，输入的数据也可能影响系统的输出和运行结果。若使用者输入的数据存在错误、虚假或侵权等问题，导致系统产生错误决策或造成损害，使用者应承担责任。例如，使用者在使用智能招聘系统时，故意输入虚假的候选人信息，导致系统做出错误的招聘决策，给企业带来损失，使用者应承担责任 。

### **●监管与行业标准遵守情况**

### ****开发者的监管责任****：开发者应遵守相关法律法规和行业标准，接受监管部门的监督检查。若开发者违反监管要求，导致人工智能系统存在安全隐患或造成损害，应承担相应责任。例如，开发者未按照数据安全法规对人工智能系统中的用户数据进行加密存储，导致数据被窃取，需承担法律责任。

### ****使用者的监管责任****：使用者在使用人工智能系统时，也需遵守相关法律法规和监管要求。若使用者因违反监管规定导致系统被滥用或造成损害，应承担相应责任。比如，使用者将人工智能客服系统用于发送垃圾信息等违法违规活动，使用者应承担法律责任 。

[5]随着AI的智能接近人类，需要考虑如何确保其安全运行，包括AI系统的可预测性和抗操纵性等。《The Cambridge Handbook of Artificial Intelligence》一书中提到，类似于法律系统的“遵循先例”原则，AI算法也需要具有可预测性，以便人们能够在其运行的环境中做出合理的决策。同时，对于一些关键应用，如机场的行李扫描系统，AI算法还需要具备抗操纵性，以防止被恶意利用.

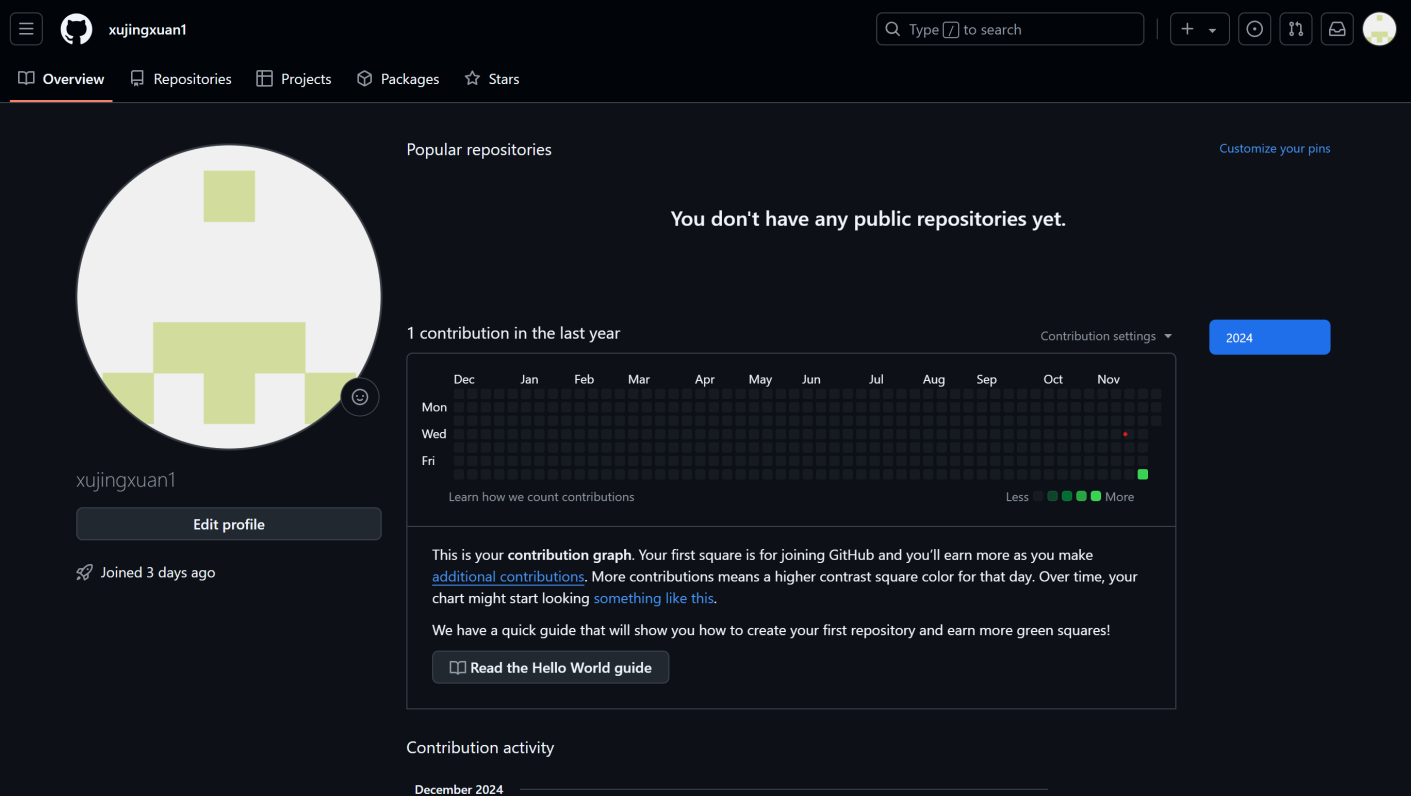
# 4 总结

# 《计算科学导论》课程是一趟知识 “奥德赛” 之旅，从计算基础启航，穿越理论迷雾，领略算法奇景，停靠应用 “港湾”，最终抵达学科前沿瞭望台。它锤炼我们逻辑思维、拓宽科技视野、点燃创新火种，为理解科技变革、投身计算领域筑牢根基。虽课程暂告段落，但开启的探索之门永不关闭，激励我们秉持计算科学 “利剑”，在未来学术、职业征途披荆斩棘，深挖计算 “富矿”，为科技进步添砖加瓦。

# 5 附录

## Github

https://github.com/xujingxuan1

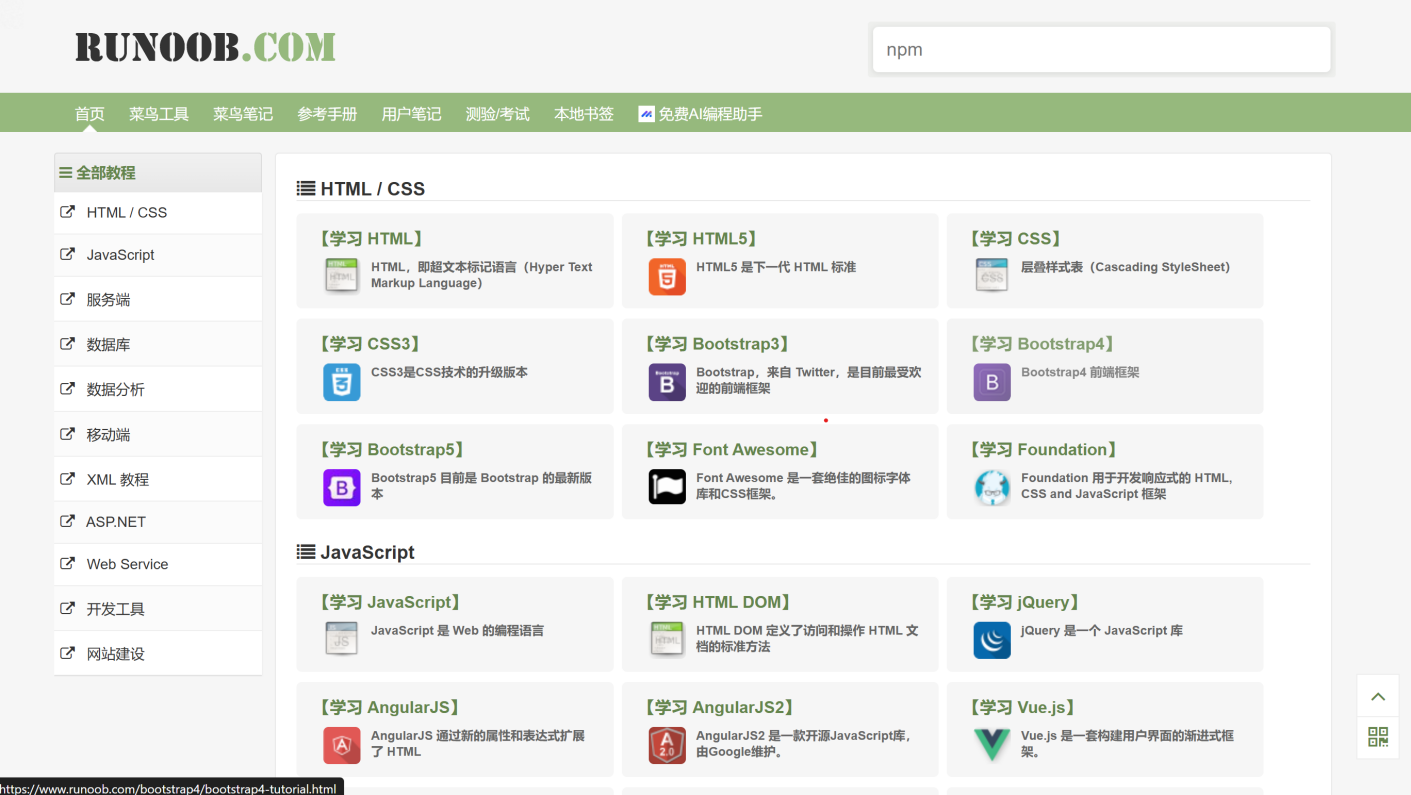


## 力扣

https://leetcode.cn/u/xjx-6x/

## 菜鸟教程

https://www.runoob.com



CSDN

https://blog.csdn.net/qwxjx\_?spm=1000.2115.3001.5343



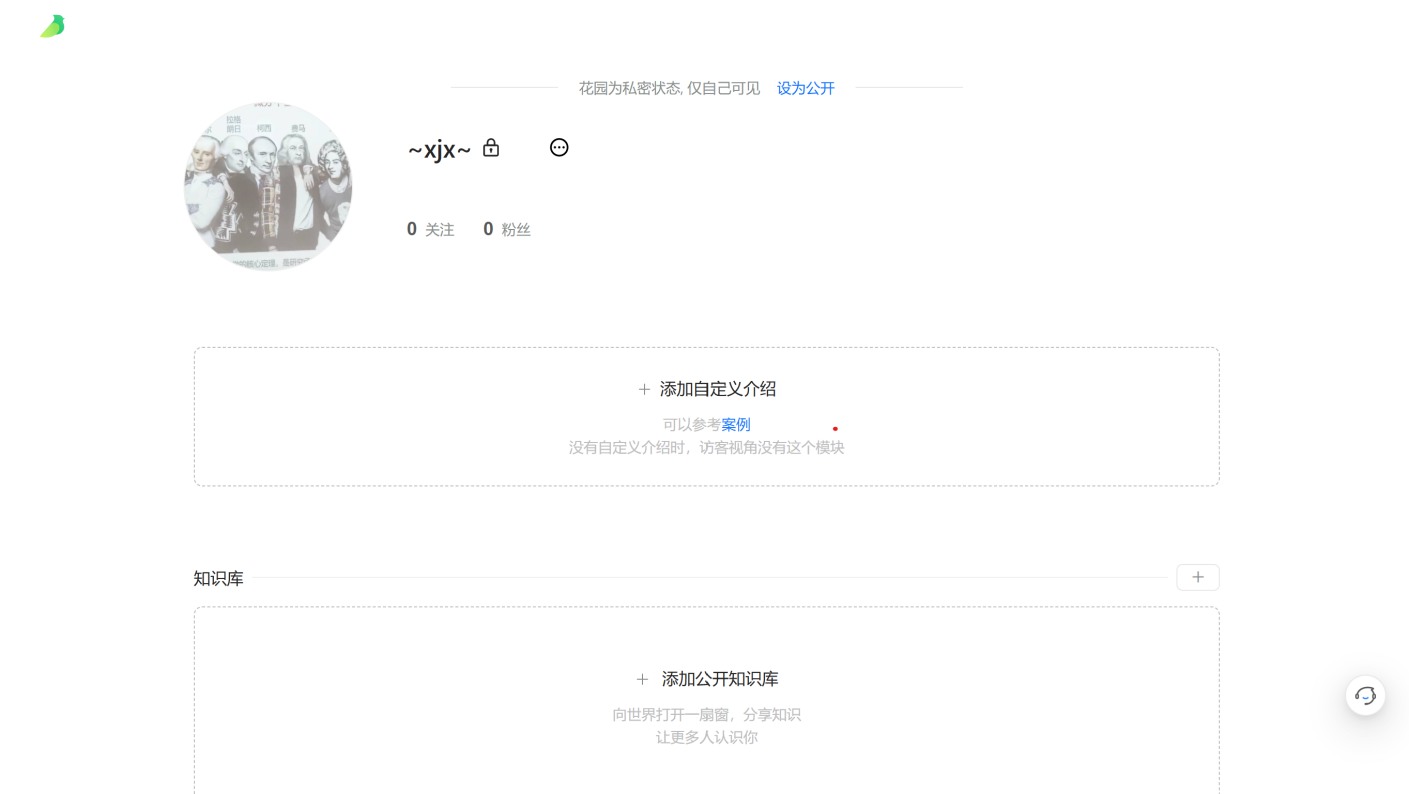
## 稀土掘金

https://juejin.cn/user/860250541132875

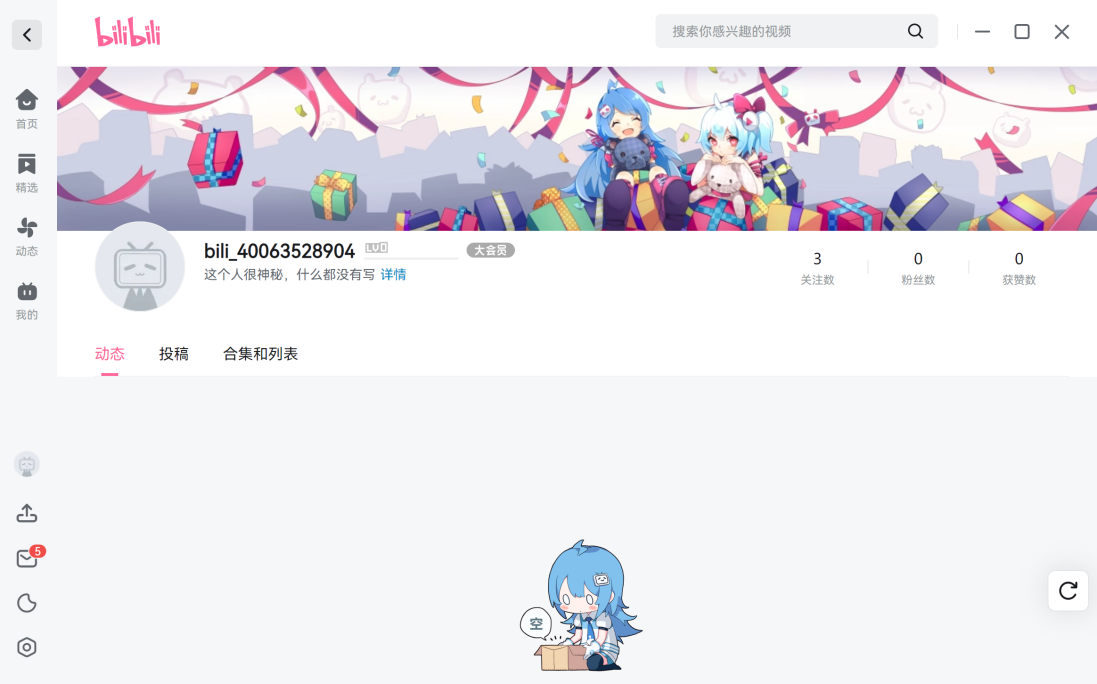


## 语雀

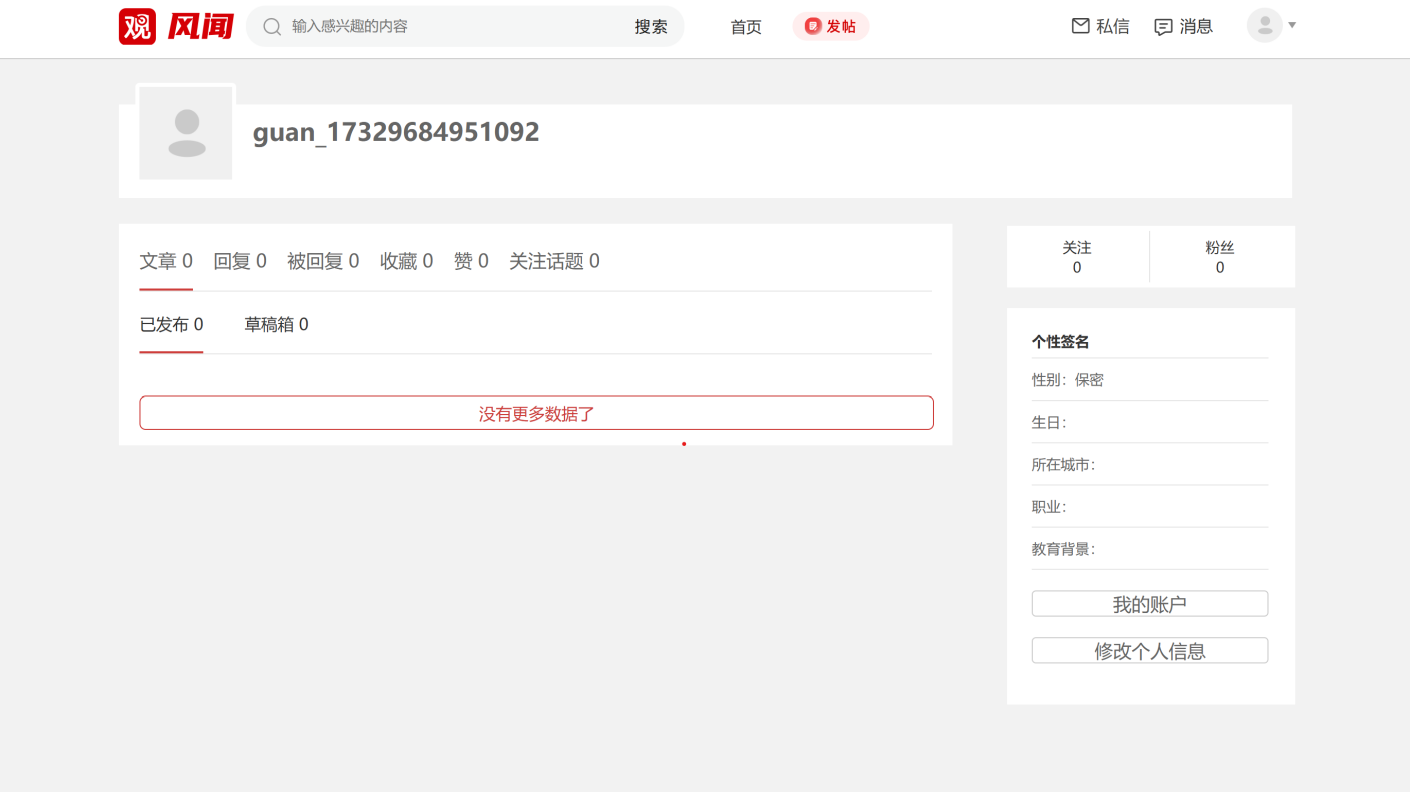
https://www.yuque.com/u49517002



## 哔哩哔哩



## 观察者



# 参考文献

[1]Michael Kozinski.Theory of Mind May Have Spontaneously Emerged in Large Language Models[J]。AI-Papers,2023.

[2]universsky.数据安全性与保护:密码学与加密技.CSDN 博客

[3]国家保密局. (2017, November 8). 数据泄露防护技术综述

[4]European Union. General Data Protection Regulation (GDPR),2016. [出版地不明]: European Union, 2016.

[5]Nick Bostrom,Eliezer Yudkowsky.The Cambridge Handbook of Artificial Intelligence[M].Cambridge University Press,2014.