

《计算科学导论》课程总结报告

学生姓名： 侯典范 学 号： 2007010211 专业班级： 计科2002 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% | Latex附加  10% | 总分 | 评阅教师 |
|  |  |  |  |  |  |  |

2021年 1月 6日

1 引言

在科学技术蓬勃发展的今天，在这个信息化逐步建立并完善的时代，计算机科学与技术正焕发出其绚烂的色彩，计算机科学与技术的应用已经渗透到整个生活。而对于作为新时代的新青年的我们，对于计算机专业的我，掌握和精通计算机科学知识，提升专业能力，为更能从容地应对“卡脖子”问题，助力我国顺利步入创新型国家行列，助力我中华民族伟大复兴和伟大中国梦的实现，乃我辈之责。通过计算科学导论的学习，我对于本专业有了初步的认识，收获了许多知识与观念。

2 对计算科学导论这门课程的认识、体会

计算科学导论这门课程是计算机科学与技术教学内容的概括，具有很强的概括性与引导性，它勾勒出计算机科学体系的一个轮廓与雏形，方便学生更清楚地认识本专业的基本方法和基本思想，从而指导后续的学习与实践。

其实我在之前对于计算机专业并没有过多的了解，选择本专业也是父母的建议和要求，所以计算科学导论这门课程对我的帮助还是很大的，让我认识到计算科学还可以上升到哲学层面，让我认识到计算科学中“科学”二字的分量。

2.1 科学哲学的思想方法

正是这节课，奠定了我以后所应采取的方法论的基础。我学到一个道理至今印象深刻——只有认识世界，才能改造世界。而如何认识世界，也就决定了你改变世界的能力。

“真正理解一件事物最好的方式莫过于去探寻它的历史”，在计算机的数学起源中，我简单了解了计算科学的历史，赞叹于先辈们做出的巨大贡献的同时，也惋惜于其中的不足，惊叹于希尔伯特公理体系的建设数学大厦的伟大构想，也唏嘘于罗素悖论使集合论产生危机而对整个公理体系造成沉重打击，哥德尔不完备定理彻底宣告将数学彻底形式化的愿望的破灭。由于对哥德尔不完备定理的不同理解，计算科学又有了新的内容。

计算科学可以追溯到20世纪30年代到60年代初，由来自数学和电子科学领域的科学家围绕什么是计算开展理论探索，后来由图灵和冯·诺依曼等人的贡献，第一台存储程序式通用电子数字计算机ENIAC于1946年诞生，从此在现代计算机系统的支持下，计算数学快速发展，随之而来的还有高级程序设计语言的发展，伴随着多领域的融合研究，计算机科学作为一个学科出现了，后又逐渐分化为计算机科学和计算机工程两大阵营，发展到现在，狭义的计算科学是计算机科学与技术一级学科，涉及对计算问题的一般研究，广义的计算科学还包括计算作为一个学科形态的所包含的学术范畴和内涵。

科学哲学与学科方法论经过了由演绎逻辑主义和逻辑经验主义到认识到其中的局限性再到如今的科学哲学和方法论的过程。它总结了科学主义的观点——认识知识的真理性应更多的考察科学方法的合理性，但不能迷信科学研究和方法，它承认了科学并不是万能的。

2.2 计算机科学的基本概念和基本知识

本章内容主要介绍了计算科学的基本概念和知识，也是由此我才接触了更多的专业名词和概念。

计算模型与二进制是计算机科学的一个基础架构，这里的计算模型的研究总脱不开形式化和形式化方法的概念，形式是事物内容存在的外在方式，形状以及结构的总和，形式化则是将事物的内容与形式分离的过程，形式化的方法则是形式化的基础上通过研究事物的形式变化规律来研究事物变化规律的全体方法的总称。例如：两个橘子和两个橘子的结合，两个梨和两个梨的结合，其形式是一样的可以抽象出来形式化运算规则 2+2=4，所谓的计算模型就是判断计算这一概念的抽象的形式系统。二进制也是计算机研制过程中的伴生品，二进制的运算规则比我们生活中的十进制要简单的多，方便了计算机的逻辑设计。此外还涉及到三进制的构想，我简单阅读了期刊论文《三进制编码实现硬件演化方法研究》，并与二进制进行了对比理解。

图灵机的出现为现代计算机的发明提供了重要思想，它的思想和原理包含了存储程序的重要思想。于是在图灵机诞生后的十年内，在冯·诺依曼为代表的一批科学家的努力下，现代存储程序式电子数字计算机基本结构和工作原理确定了下来。由存储器、运算器、控制器、输入设备和输出设备组成。

数字逻辑是应用数字电路进行数字系统逻辑设计。其实电子数字计算机是由具有各种逻辑功能的逻辑部件组成的，这些逻辑部件按结构可分为组合逻辑电路（由与门、或门、和非门等门电路组合）和时序逻辑电路（由触发器和门电路组成）。对组合逻辑电路和时序逻辑电路进行合理设计和安排便可以表示和实现布尔代数的基本运算。总之，真正构成计算机科学基本内容的是围绕计算而展开的的大量带有规律性的知识，而不是具体的实现技术。

机器指令与汇编语言，计算机系统的计算能力是由基本指令系统决定，即指令决定计算系统的计算能力。而使用过程中指令系统的缺陷逐渐显现，大量的硬件设计和译码、存储和寻址等开销的增大迫使指令系统亟需改进。研究员在尝试改进的过程中，认识到了应该公平对待硬件和软件的地位，使两者平衡负担整个系统的复杂性。精简指令系统计算机（RISC）由此诞生。RISC实质上是一种体系结构设计的思想，由于它极大地提高了计算机的运算速度，被誉为计算机体系结构发展史上的一个里程碑。汇编语言则是由一组汇编指令构成的语言，由各字符串的缩写代表操作，用符号代表数据的二进制、八进制和十进制的数字序列。汇编程序是编写和设计汇编语言翻译程序，负责把使用的汇编语言书写的程序翻译成可直接执行的机器指令程序。但是，汇编语言在可读性和编写时并不能让人满意，这导致了高级程序设计语言的进一步发展。

2.3 计算科学的意义、内容和方法

计算科学是对描述和变换信息的算法过程，包括其理论、分析、设计、效率分析、实现和应用的系统研究。

计算科学的问题域包括数值模拟、模型拟合与数据分析计算优化等领域，其基本问题是什么能有效地自动进行，什么不能有效地自动进行。计算已经成为继理论、实验之后的第三种科学形态。当我们今天以科学哲学的观点对学科进行回顾和系统总结时，我们发现学科研究与发展普遍关心的基本问题有三个，即计算的平台与环境问题、计算过程的能行操作与效率问题还有计算的正确性问题。理论研究中提出的各种计算机体系结构，各种软件开发工具与环境，编译程序与操作系统，数据库系统等都是围绕计算的平台与环境问题这一基本问题展开，其内容实质为计算模型问题。而围绕计算过程的能行操作与效率问题，大量例如数值与非数值计算方法，算法设计与分析，结构化程序设计技术与效率分析，人工智能的逻辑基础等研究内容和分支学科方向得到发展，这一基本问题是的核心是算法问题。围绕计算的正确性问题学科发展了例如算法理论、程序理论、程序设计语言的语义学等等，计算的正确性问题可归结为语义学问题。

通过对计算模型与计算机的学习，我也试想了不同于电子计算机形式的计算机，并阅读了期刊论文《计算机科学与技术的应用现状与未来趋势分析》，简单了解了生物计算机、量子计算机、光子计算机以及纳米计算机的未来发展与趋势。

3 进一步的思考

在课程的分组演讲中，我们小组选择的课题是“拜占庭将军问题”。在研究与演讲的过程中，我们对其基本概念，内涵，发展以及应用进行了初步的探索。

3.1 拜占庭将军问题的基本概念和发展史

拜占庭将军问题是由莱斯利·兰伯特提出的点对点通信中的基本问题。含义是在存在消息丢失的不可靠信道上试图通过消息传递的方式达到一致性是不可能的。我们对其的理解是，古老的拜占庭帝国有若干支军队，每支军队都分隔很远，将军与将军之间只有通过派遣信使才能传递消息，而若想取得战争的胜利，必须让所有军队达成共识，但是军队内部可能出现内奸篡改和伪造信息，阻止共识的达成，这样，在已知存在内奸的情况下如何达成一致的协议，拜占庭将军问题由此产生。拜占庭假设是对现实世界的模型化，由于硬件错误、网络拥塞或断开以及遭到恶意攻击，计算机和网络可能出现不可预料的行为。

拜占庭将军问题于1982年由莱斯利·兰伯特提出，并于同年得出结论——在内奸数量大于等于三分之一的情况下，拜占庭将军问题不可解。1999年，Miguel Castro和Barbara Liskov提出了实用拜占庭容错算法（PBFT），实现了在内奸不超过三分之一的情况下使忠诚的将军达成一致的结果。2009年中本聪发明了比特币，为拜占庭将军问题提出来新的解决之道。

3.2 实用拜占庭容错算法（PBFT）

实用拜占庭容错算法中，我们简单研究了PBFT机制是如何运行的，并清楚了其运行过程与反馈机制，加以形象化的表述。

其具体运行过程如下图所示：

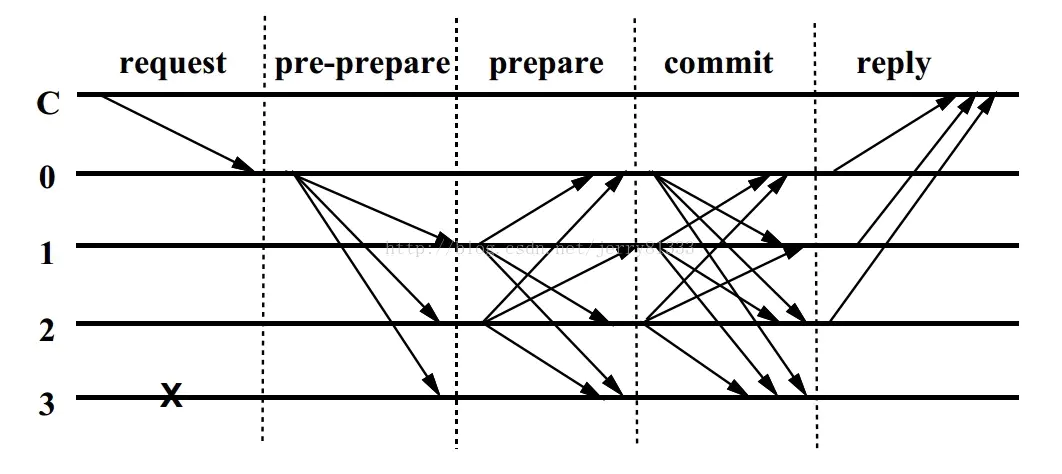


图 1： PBFT流程

在非主节点失效的情况下，先进行client请求阶段。总司令给军长下命令。

预准备（pre-prepare）阶段：主节点向所有backup节点发送预准备消息，其中包括当前视图编号，client请求以及请求摘要，签名是否一致等。军长对各位师长说：现在是我被委任为军长（视图），你们都是师长，所有人都得听我的。现在公布总司令的命令（先说说总司令是谁，命令摘要）。  
准备(prepare)：包括主节点在内的所有副本节点在收到准备消息之后，对消息的签名是否正确，视图编号是否一致，以及消息序号是否满足水线限制这三个条件进行验证，如果验证通过则把这个准备消息写入消息日志中。backup节点核对签名信息，比如其他师长听到总司令的名字，说对，总司令就是这个人没错，然后核对总司令曾经任命这个人当军长，好吧，那就听他的吧。  
确认(commit)：每个副本接受确认消息的条件是：1）签名正确；2）消息的视图编号与节点的当前视图编号一致；3）消息的序号n满足水线条件，在h和H之间。一旦确认消息的接受条件满足了，则该副本节点将确认消息写入消息日志中。每个师长都经过上述核对，确认无误，就会接受命令进行执行。  
回复（reply）：结果反馈。

预准备和准备两个阶段用来确保同一个视图中请求发送的时序性（即使对请求进行排序的主节点失效了），准备和确认两个阶段用来确保在不同的视图之间的确认请求是严格排序的。

PBFT算法的核心理论是n>=3f+1  
n是系统中的总节点数，f是允许出现故障的节点数。换句话说，如果这个系统允许出现f个故障，那么这个系统必须包括n个节点，才能解决故障。这也是之前提到的内奸不超过三分之一的条件。

3.3 比特币

2009年，中本聪提出的比特币为拜占庭将军问题提出了新的解决方案。比特币中的POW工作量证明机制规定，一段时间内只能有一位将军发出消息，而这个发出消息的将军为率先解决出复杂的数学问题的将军。当其他将军收到统一发出的消息时，必须签名盖章来确认各自的身份，再反馈给其他将军，这里的签名方式是不可伪造、不可篡改的，即采取非对称加密，这样，如果内奸要破坏统一的命令，就必须让51%的将军都变成叛徒，这样大大增加了成本，即51%攻击。而在现实世界中，做到51%攻击几乎不可能，并且如果真的掌握了51%算力，其挖矿维护网络所获得的收益远远高于其破坏网络所取得的收益。

共识算法之POW，是目前被较多区块链系统应用的共识算法，规定，每轮完成海量哈希计算并最先给出正确答案的唯一一个节点获胜，获得挖矿奖励，POW实质考察的是算力。其安全性能高，若想破坏和篡改此系统，要具备全网51%以上的算力才可以。

非对称加密，在区块链系统里，每个人都有两把钥匙——公钥和私钥，私钥能生成公钥和地址，私钥加密，公钥解密。首先是买家对明文进行哈希加密，得到64位的字符串，接着买家用私钥再次加密获得另一个字符串A，卖家对字符串进行哈希计算，再通过买家提供的公钥解密数字签名，得到字符串B,当字符串A、B的哈希值一致，公钥和私钥能够成功配对，才可证明交易信息为真。

3.4 拜占庭将军问题的发展趋势

拜占庭将军问题最直接的发展趋势便是去中心化的网络，而区块链的两大最显著的特点便是去中心化与分布式记账。区块链无疑成为了拜占庭将军问题最适合的用武之地。很显然，实用拜占庭容错算法（PBFT）为区块链系统运行提供了巨大的帮助，也是密码学中“多数人共识”的主要获得方式，在今后的发展中，PBFT（实用拜占庭容错算法）、POW（工作量证明机制）、POS（权益证明机制）、DPOS（委托权益证明机制）、POSpace（容量证明机制）和POI（重要性证明机制）等协同工作，相互配合会使区块链系统运行的效率更高，安全性更强。

4 总结

总体来说，计算科学导论这门课程对我的帮助和启发还是很大的，这门课程让我由一位什么都不懂的计算机小白逐渐变得入门了，也接触了很多的专业名词并对此进行了记忆和理解，有些概念和结论在阅读后有了默认的理解，期待在以后的学习中能对这些概念有新的认识和深入的理解以致有独到的见解。计算科学导论的目录就是我今后对专业学习的框架，它会帮助我整理和完善整套的知识体系。

5 附录

· Github

个人主页 <https://github.com/Scandinavia20>

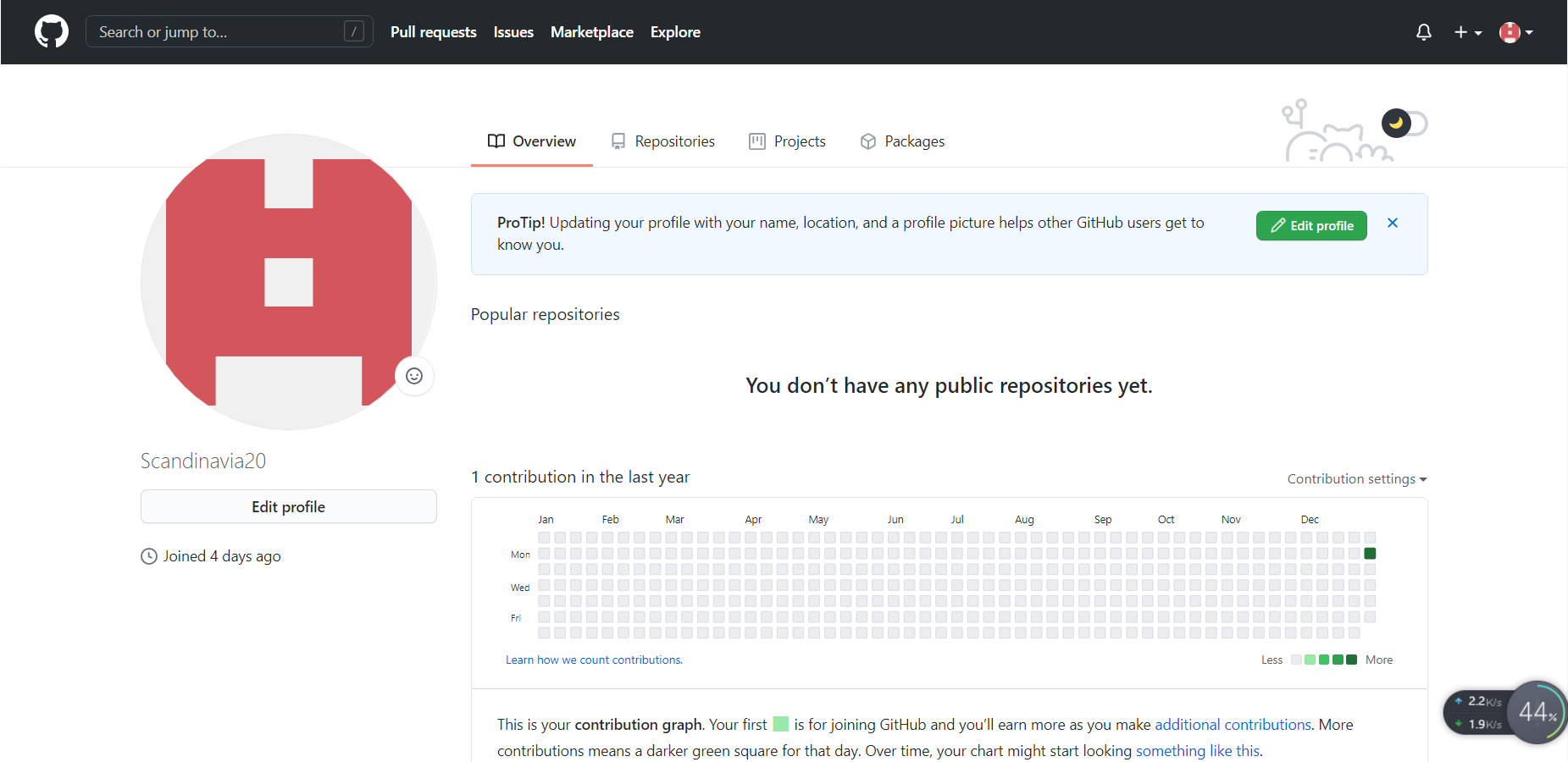


图 2：Github个人主页

·观察者、学习强国、哔哩哔哩



图 3：观察者网



图 4：学习强国



图 5： 哔哩哔哩

·CSDN、博客园

CSDN个人主页 <https://blog.csdn.net/qq_51579409?spm=1010.2135.3001.5343>

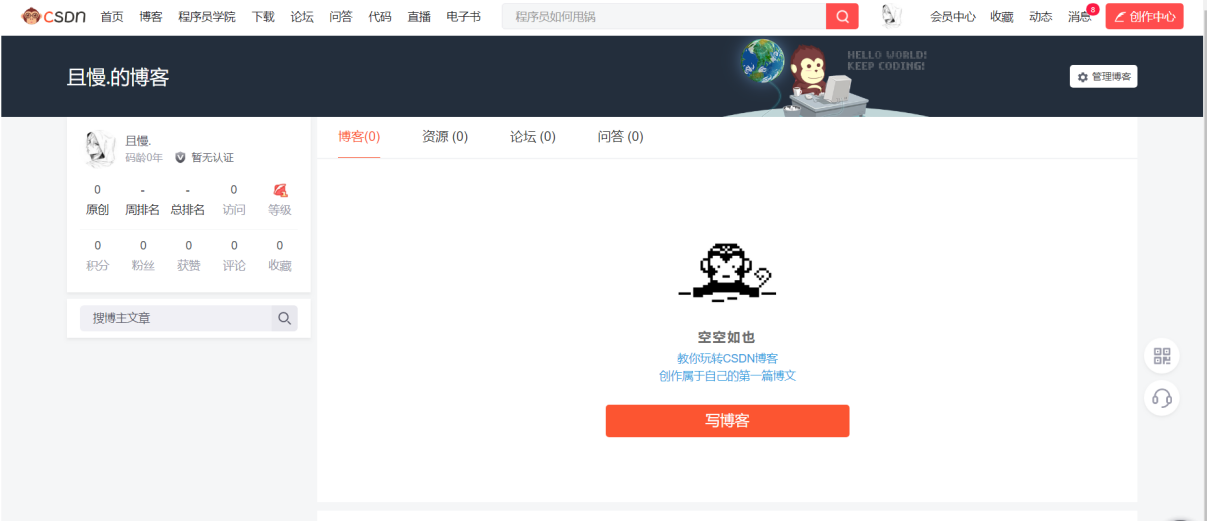


图 6：CSDN

博客园个人主页 <https://home.cnblogs.com/u/2275104/>

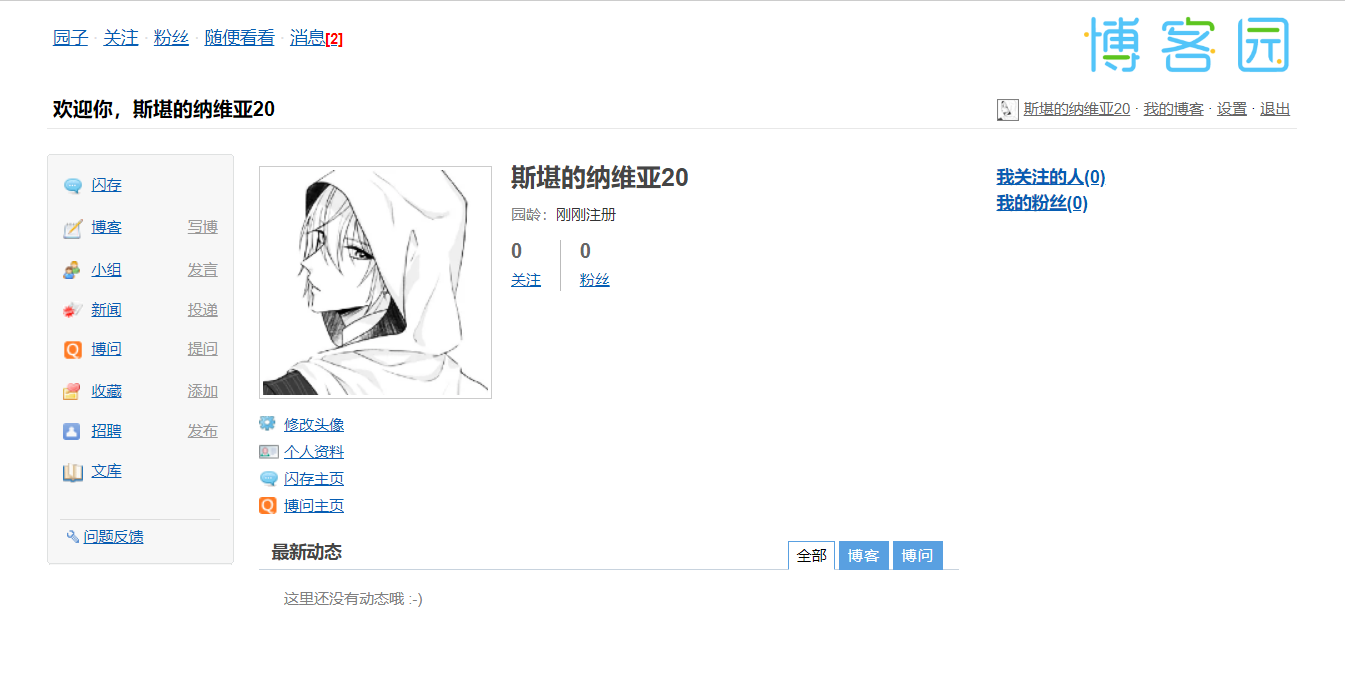


图 7：博客园

·小木虫

个人网址 <http://muchong.com/bbs/space.php?uid=24941029>



图 8：小木虫

参考文献

1. 张浩. 基于相变存储器的三进制计算研究[D].华中科技大学,2019.
2. 王灏.计算机科学与技术的应用现状与未来趋势分析[J].无线互联科技,2020,17(21):66-67+70.
3. 孙耀景. 基于实用拜占庭容错算法的区块链共识算法研究[D].湘潭大学,2020.

[4] Junxing Wang. A simple Byzantine Generals protocol. 2014, 27(3):541-544.

[5] Quality-by-Design-engineered pBFT Consensus Configuration for Medical Device Development.[J]. Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual International Conference,2020,2020.