

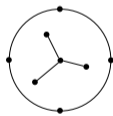
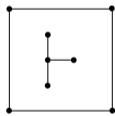
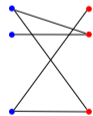
Computational Complexity

傅育熙，上海交通大学

Let's take a look at some familiar problems.

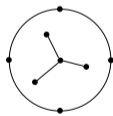
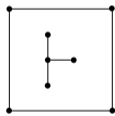
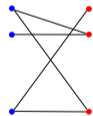
1. Diophantine Problem
2. Matching Problem
3. Graph Isomorphism Problem
4. Vertex Cover Problem

整数方程 $a_1x_1^{n_1} + a_2x_2^{n_2} + \dots + a_kx_k^{n_k} = 0$



We learnt from the **Computability Course** and the **Algorithm Course** that

1. Diophantine Equation $a_1x_1^{n_1} + a_2x_2^{n_2} + \dots + a_kx_k^{n_k} = 0$ is undecidable,
2. Matching is in **P**,
3. Graph Isomorphism is yet to be classified, and
4. Vertex Cover is **NP**-complete.



This course is about **classifying** and **comparing** problems by the amount of resource necessary to solve them.

We shall get to know some of the main techniques in theoretical investigations.

- ▶ Algebraic Method
- ▶ Probabilistic Method
- ▶ Combinatorial Method

计算理论中的证明会用到递归论的、算术的、组合的、代数的、概率的、统计的、图论的、数论的、信息论的、博弈论的、证明论的、纠错码理论的方法

We shall be exposed to quite a few great ideas in Computer Science.

Blum's Speedup Theorem, Borodin-Trakhtenbrot Gap Theorem, **BPP**, Hierarchy Theorem, Savitch Theorem, Stockmeyer-Meyer Theorem, **NC**, Karp Theorem, Cook-Levin Theorem, **PH** \subseteq **PSPACE**, Baker-Gill-Solovay Theorem, Immerman-Szelepcsényi Theorem, **DistNP**, Ladner Theorem, Circuit Complexity, Chandra-Kozen-Stockmeyer Theorem, PCP Theorem, **P**-Completeness, Aleliunas-Karp-Lipton-Lovász-Rackoff Theorem, **PP**, Valiant Theorem, $\#\mathbf{P}$, Valiant-Vazirani Theorem, Toda Theorem, Impagliazzo-Levin Theorem, Adleman Theorem, Goldbach-Levin Theorem, NP-Completeness, Zero Knowledge, Yao's Unpredictability Theorem, Lund-Karloff-Fortnow-Nisan Theorem, Yao's Max-Min Theorem, Derandomization, **AM**, Barrier Results, Goldbach-Goldwasser-Micali Theorem, Pseudorandomness, One-Way Function, Nisan-Wigderson Generator, **IP** = **PSPACE**, Hartmanis Conjecture, Hardness Amplification, Hierarchy Theorem, Exponential Conjecture, Sudan's List Decoding, **RP**, Reingold Theorem, Hartmanis-Stearns-Hennie Theorem, Goldwasser-Sipser Theorem, Randomness Extractor, **QIP** = **PSPACE**, Log-Rank Conjecture, Circuit Lower Bound, Levin Theory, Natural Proof, hardness of approximation, communication complexity, **BQP**, Håstad Switching Lemma, Circuit Hierarchy Theorem, ...

伟大的思想都在伟大的证明里，伟大的技术都在伟大的应用中

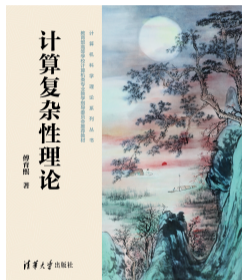
In Part I we discuss

efficient computation.

In Part II we study hard problems using a combination of ideas that can be summarized as

“randomization + interaction + error”.

教材



理想

过程

现实



船只 \Rightarrow 传智 \Rightarrow 智慧 \Rightarrow 教育

《计算机专业教育丛书》，基础理论系列

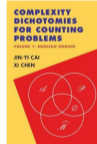
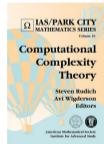
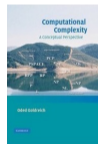
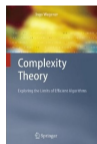
主任：傅育熙

编委（按姓氏笔画排序）

1. 王小云，清华大学
2. 邓玉欣，华东师大
3. 尹一通，南京大学
4. 孙晓明，中科院计算所
5. 李昂生，北京航空航天大学
6. 李 建，清华大学
7. 陈翌佳，上海交通大学
8. 陆品燕，上海财经大学
9. 邱道文，中山大学
10. 郁 昱，上海交通大学
11. 张志华，北京大学
12. 张立军，中科院软件所
13. 姚期智，清华大学



1. C. Papadimitriou. Computational Complexity. 1994.
2. I. Wegener. Complexity Theory, exploring the limits of efficient algorithms. 2005.
3. O. Goldreich. Computational Complexity, a conceptual perspective. 2008.
4. S, Arora, B. Barak. Computational Complexity, a modern approach. 2009.
5. A. Wigderson. Mathematics + Computation, a theory revolutionizing technology and science. 2020.



成绩 = 练习 (50) + 期终考试 (50)

为什么这门课日益重要？

你能从这门课里获得的是人类智慧

课程主页: <https://basics.sjtu.edu.cn/~yuxi/teaching/complexity/>