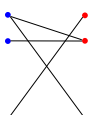
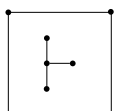
Computational Complexity

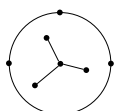
Let's take a look at some familiar problems.

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

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

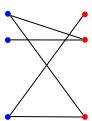


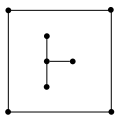


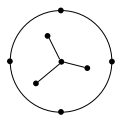


We learnt from the Computability Course and the Algorithm Course that

1. Diophantine Equation $a_1 x_1^{n_1} + a_2 x_2^{n_2} + \ldots + a_k x_k^{n_k} = 0$ is undecidable,
2. Matching is in $\mathbf{P}$,
3. Graph Isomorphism is yet to be classified, and
4. Vertex Cover is $\mathbf{NP}$-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, $\mathbf{BPP}$, Hierarchy Theorem, Savitch Theorem, Stockmeyer-Meyer Theorem, $\mathbf{NC}$, Karp Theorem, Cook-Levin Theorem, $\mathbf{PH} \subseteq \mathbf{PSPACE}$, Baker-Gill-Solovay Theorem, Immerman-Szelepcsényi Theorem, $\mathtt{Dist}\mathbf{NP}$, Ladner Theorem, Circuit Complexity, Chandra-Kozen-Stockmeyer Theorem, PCP Theorem, $\mathbf{P}$-Completeness, Aleliunas-Karp-Lipton-Lovász-Rackoff Theorem, $\mathbf{PP}$, Valiant Theorem, $\sharp\mathbf{P}$, Valiant-Vazirani Theorem, Toda Theorem, Impagliazzo-Levin Theorem, Adleman Theorem, Goldreich-Levin Theorem, NP-Completeness, Zero Knowledge, Yao's Unpredictability Theorem, Lund-Karloff-Fortnow-Nisan Theorem, Yao's Max-Min Theorem, Derandomization, $\mathbf{AM}$, Barrier Results, Goldreich-Goldwasser-Micali Theorem, Pseudorandomness, One-Way Function, Nisan-Wigderson Generator, $\mathbf{IP} = \mathbf{PSPACE}$, Hartmanis Conjecture, Hardness Amplification, Hierarchy Theorem, Exponential Conjecture, Sudan's List Decoding, $\mathbf{RP}$, Reingold Theorem, Hartmanis-Stearns-Hennie Theorem, Goldwasser-Sipser Theorem, Randomness Extractor, $\mathbf{QIP} = \mathbf{PSPACE}$, Log-Rank Conjecture, Circuit Lower Bound, Levin Theory, Natural Proof, hardness of approximation, communication complexity, $\mathbf{BQP}$, 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

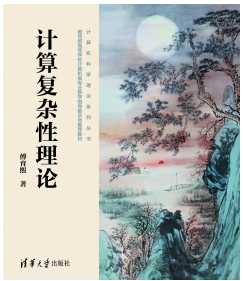
In Part I we discuss

efficient computation.

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

"randomization + interaction + error".

教材



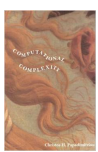
理想

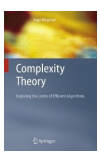
过程

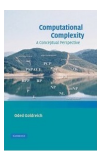
现实

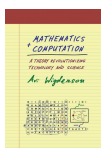
传智（船只）⇒ 教育

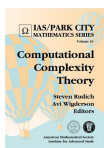
1. C. Papadimitriou. Computational Complexity. 1994.
2. I. Wegener. Complexity Theory, exploring the limits of efficient algorithms. 2005.
3. O. Goldreich. Computational Complexity, a conceptual perspective. 2008.
4. S, Arora, B. Barak. Computational Complexity, a modern approach. 2009.
5. A. Wigderson.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

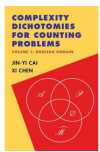












为什么这门课日益重要？

成绩 = 练习 (50) + 期终考试 (50)