离散数学 (荣誉)

Discrete Mathematics (Honor)

2023 Fall

殷翔

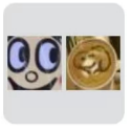
September 15, 2023

Instructor Information

- Name: 殷翔
- Affiliation: 电院 自动化系
- Title: 副教授，博导，国家青年千人
- Contact: yinxiang@sjtu.edu.cn Wechat!
- Office: 电院2号楼 443
- Education:
  - ✓ Bachelor from the Zhejiang University (2012)
  - ✓ PhD from the University of Michigan (2017)
- Research: control theory, theoretical computer science

Course Information

- Credit: 3 credits / 48 hours
- Grading:
  - ✓ Homework Assignments: 25%
  - ✓ In Class Quiz: 15% (three times)
  - ✓ Final Exam: 60% (closed book)
- Textbooks:
  - ✓ My course notes!
  - ✓ 数理逻辑与集合论，石纯一等，清华大学出版社
  - ✓ 图论与代数结构，戴一奇等，清华大学出版社
  - ✓ Discrete Mathematics and Its Applications, K. H. Rosen, McGraw Hill.
- Working Language: English & Chinese
- Question after class or by Wechat or by appointment
- Teaching Assistant: 陈煜



群聊：2023秋-离散数学-致远学院

Syllabus

Part I: Mathematical Logics (数理逻辑)---Week 1-6

- Propositional Logics (命题逻辑)
- Predicate Logics (谓词逻辑)
- Axiomatic Systems (公理系统)

Part II: Set Theory (集合论)---Week 7-12

- Naïve Set Theory (朴素集合论)
- Axiomatic Set Theory (公理集合论)
- Relations and Functions (关系与函数)

Part III: Graph Theory (图论)---Week 13-16

- Paths, Trees, Euler/Hamilton Graphs...

Main Purpose of This Course

- 离散数学的最大特点是“散”：研究散的东西，覆盖面散
- 推理过程、计算机执行都是一步一步的，不是连续的
- 技术目标：熟悉各类逻辑运算、离散算法，掌握严格的数学证明
- 思想目标：掌握形式化演绎的思想，构建抽象逻辑推理的能力
- Discrete Math is the foundation of EECS!
  - 数据结构、算法设计、操作系统、编程语言
  - 数字电路、电路拓扑、自动控制密码学
  - 信息论、通信理论
  - 专家系统、知识图谱、神经网络

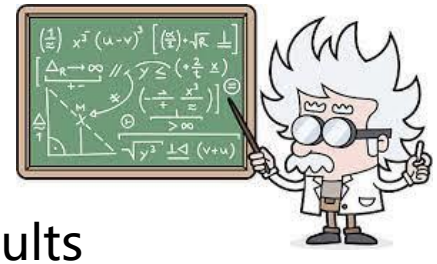
How Do Humans Acquire Knowledge?

Approach 1: Inductive (归纳)

- Start from your observation and experiment
- Summarize and verify if it explains what you see
- Example: Newton discovered the laws of gravity

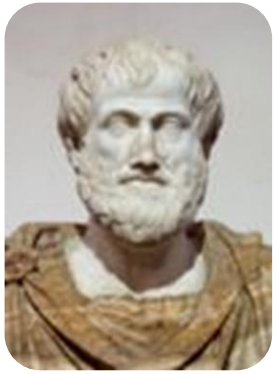
Approach 2: Deductive (演绎/推理)

- Start from some basic common knowledges
- Use some basic deduction rules to get new results
- Example: Einstein discovered the theory of relativity



This course is mostly about how to reason correctly

Formal Reasonings



亚里士多德 Aristotle (384BC-322BC)

- The founder of formal logic, the first logician
- Syllogism (三段论): first formal logic system

An Example of Syllogism

Major Premise: SJTUers are smart

\+

Minor Premise: You are a SJTUer

=

Conclusion: You are smart!

Formal Reasonings

Reasoning has to start from some basic points you cannot prove

- 天亮←太阳发光←元素聚变←质子/中子重组←基本粒子/夸克←more?
- How do you know what you believed is still correct tomorrow? Never!
- But you can make conditional reasoning: if A holds, then we have B
- Those you believe but cannot prove are called axioms (公理)

Otherwise you will fall into circular reasoning (循环论证)

- Example 1:
  - 你为什么长得胖？因为我吃得多
  - 那你为什么吃得多？因为我长得胖

- Example 2:
  - 圣经说神（一种永远正确的东西）存在
  - 由于圣经是神说的，所以必然正确无误

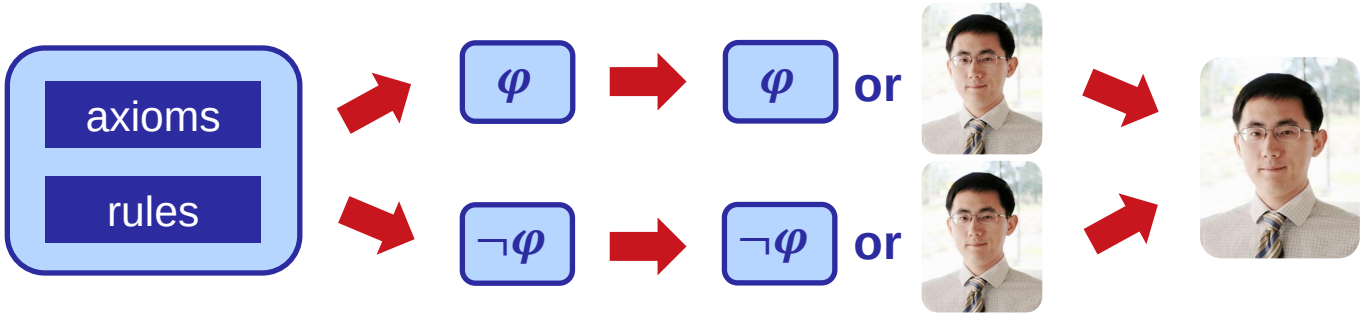
Axiomatic System

Axiomatic System = Basic Axioms + Derivation Rules

- each axiom needs to be independent (独立的)
- an AS is said to be consistent (一致的) if has no contradiction
- an AS is said to be complete (完备的) if every statement is capable of being proven true or false

What if an axiomatic system is NOT consistent

- Then you can "prove" whatever you want!



The First Axiomatic System

欧几里得 Euclid (325BC-265BC)

- "Euclid's Elements" (几何原本)
- describes an axiomatic system based on definitions and five postulates (axioms)

欧氏几何的五条公理

① 过两点能作且只能作一直线

② 线段(有限直线)可以无限地延长

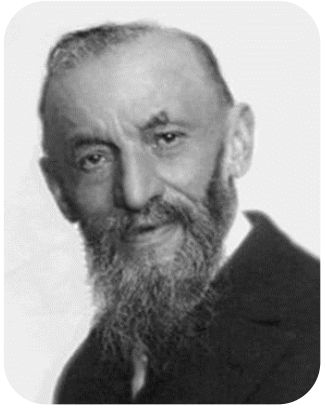
③ 以任一点为圆心,任意长为半径,可作一圆

④ 凡是直角都相等

⑤ 通过一个不在直线上的点，有且仅有一条不与该直线相交的直线

Other Axiomatic Systems

Peano Axioms 皮亚诺公理 (一阶算数系统)



① 0是自然数

② 任何自然数都有一个后继数，它也是个自然数

③ 任何自然数的后继数都不是0

④ 对任意两个自然数a和b，如果a的后继数和b的后继数是同一个数，那么a和b是同一个自然数

⑤ 假设某命题对自然数0成立。且，当该命题对自然数n成立时，可以证明该命题对n的后继数也成立。由前两句话就可得出，该命题对所有自然数成立。

$$0 \xrightarrow{S} 1 \xrightarrow{S} 2 \xrightarrow{S} 3 \xrightarrow{S} \dots$$

Axioms are What You Believe or Based On

Axiom is like your Girlfriend:

- either you accept that all she says are correct
- or you choose to have a new one…
- In any case, you cannot argue with the axioms

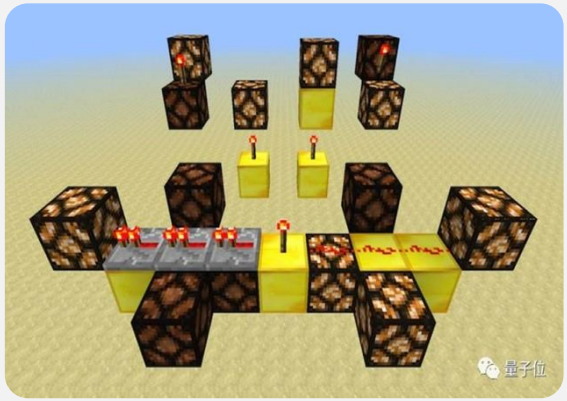
Sometimes you will find a new world by changing axioms

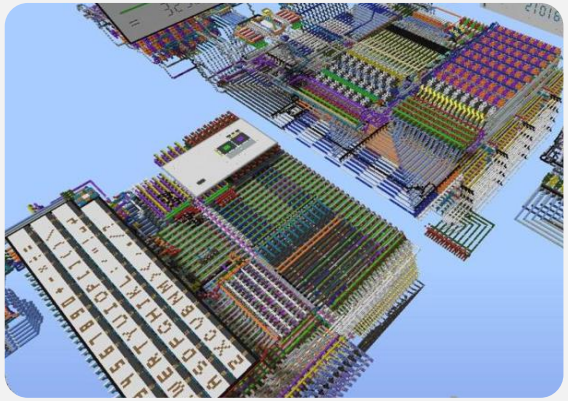
- 不接受平行公设：罗巴切夫斯基→非欧几何
- 罗氏几何 (双曲几何)：可以引最少两条平行线→内角和小于180
- 黎曼几何 (椭圆几何)：一条平行线也不能引→内角和大于180
- 不接受牛顿定律：相对论...

The Powerfulness of Axiomatic Systems

- 正常人玩法：

- 大神的玩法：



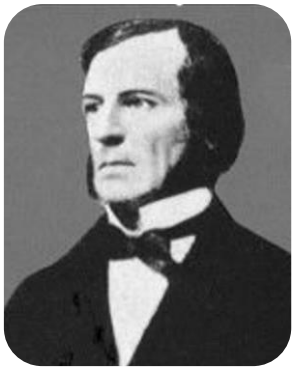


简单造就复杂：道生一，一生二，二生三，三生万物

Logics are Just Symbols

莱布尼茨 Gottfried Leibniz (1646-1716)

- First time use “Mathematical Logic”
- Leibniz’s Dream: Reasoning is essentially symbolic computation
- He proposed “universal characteristic” and said “Let us calculate”

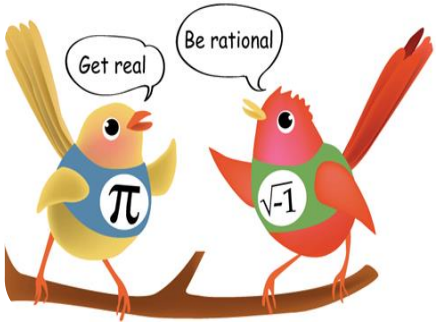


布尔 George Boole (1815-1864)

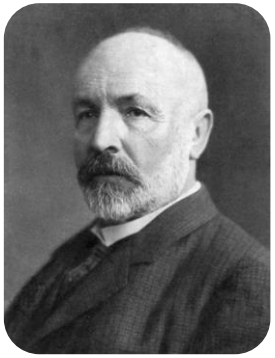
- Boolean algebra (布尔逻辑): first time to use math to study logic
- Set algebra or switching algebra
- now is already the basis of computer science

Understanding Infinity

- First Mathematical Crisis:
  Greeks thought all number are rational q/p until found $\sqrt{2}$
- Second Mathematical Crisis:
  What is limit? Is infinitely small equals to zero?
- Are infinities the same?
  Which infinity is larger: even numbers/natural number, real number/rational number



- Surprisingly, these very fundamental questions are answer very late in 1800s based on the real number theory and the set theory



康托尔 Georg Cantor (1845-1918)

- Built the set theory as the foundation of mathematics
- People realize infinities are actually different
- 庞加莱于1900年国际数学家会议上夸耀道:
  现在可以说（数学）绝对的严密性是已经达到了

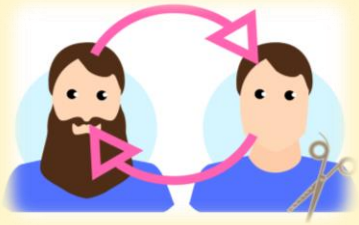
Russell's Paradox

罗素 Bertrand Russell (1872-1970)

- naive set theory→ axiomatic set theory
- He thinks all mathematics should be derived from logic!
- "Principia Mathematica"《数学原理》with Whitehead

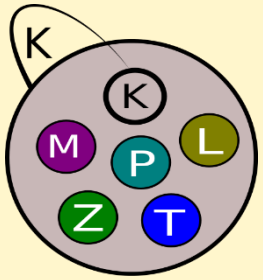
理发师悖论

- 社区里有个理发师，制定了以下规矩：
  他只给不给自己理发的人理发
- 问题：他给不给自己理发?
- 如果他不给自己理，
  那么他要给自己理
- 如果他给自己理，
  那么他不能给自己理



罗素悖论

- 所有不属于自身的元素构成的集合，
  i.e., $K = \{x \mid x \notin x\}$
- Questions: $K \in K$ or $K \notin K$?
- If $K \in K$,
  then $K \notin K$
- If $K \notin K$,
  then $K \in K$



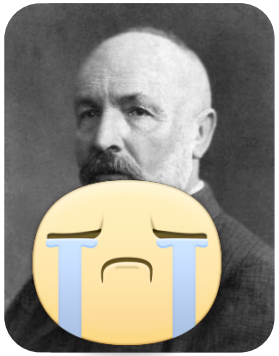
Axiomatic Set Theory

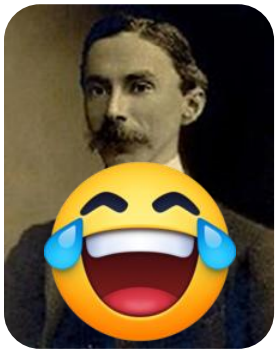
Naïve Set Theory (朴素集合论)

- proposed by Cantor
- Basic Idea:
  anything you can describe is a set
- helped people to understand infinity
- its logic foundation is questionable

Axiomatic Set Theory (公理集合论)

- first axiomatic set theory by Zermelo
- becomes the classical ZF-set theory by Fraenkel (1922)
- Basic Idea:
  you can only construct a new set based on some existing sets and some rules





Axiomatic set theory is now the foundation of the entire mathematics

Hilbert's Dream

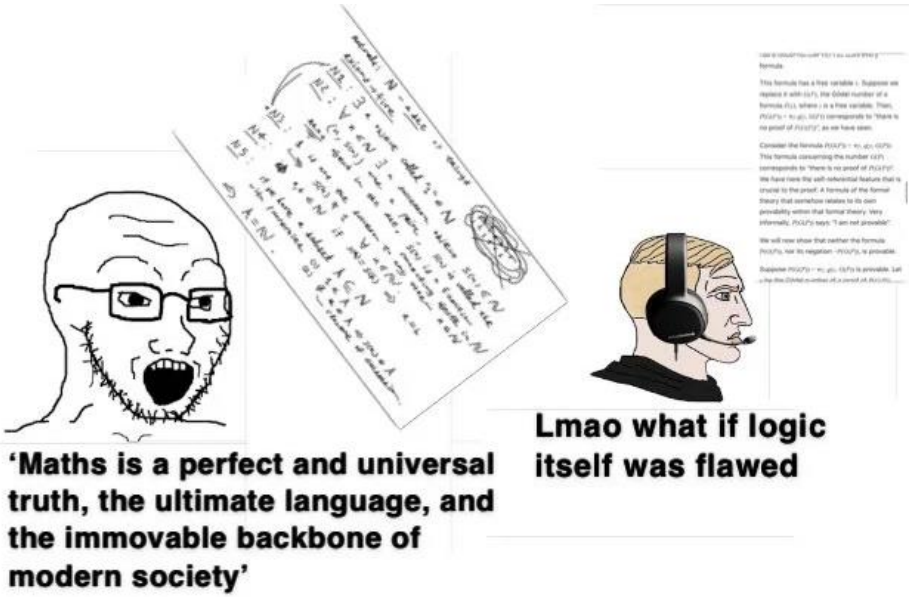
希尔伯特 David Hilbert (1862-1943)

- The founder of the proof theory
- He wanted mathematics to be formulated on a solid and complete logical foundation: both complete and consistent

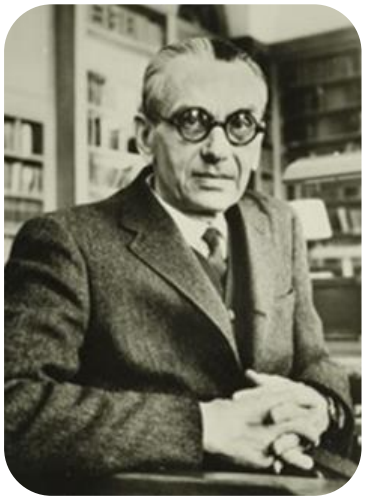
Hilbert's Program

① all of mathematics follows from a correctly chosen finite axiom system

② such axiom system is provably consistent through some means



Gödel's Incompleteness Theorems



哥德尔
Kurt Gödel
(1906-1978)

哥德尔第一不完备定理 (1931)

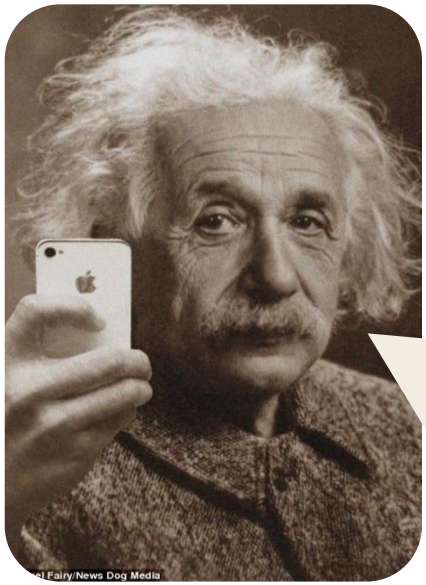
- Any powerful enough (supports Peano arithmetic) consistent axiom system must has a true proposition that cannot be proved
- 解读：不存在一个万能的公理系统，使得其既能够证明一切数学真理，又能证伪任何谬误

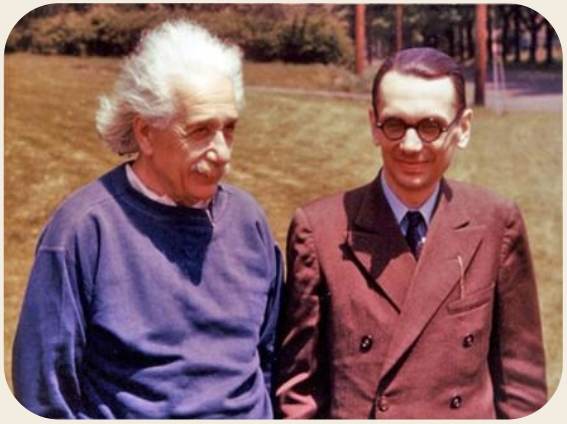
哥德尔第二不完备定理(1931)

- Any powerful enough consistent axiom system cannot prove its own consistency
- 解读：如果一个（强度足以证明基本算术公理的）公理系统可以用来证明它自身的一致性，那么它是不一致的。

Gödel's incompleteness theorems show Hilbert's Program is NOT POSSIBLE!

About Gödel

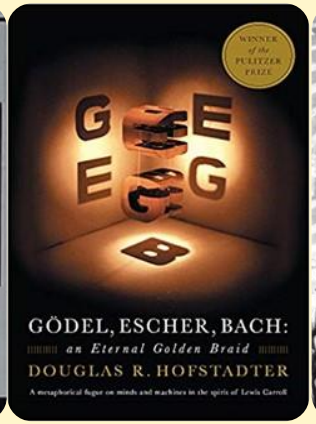


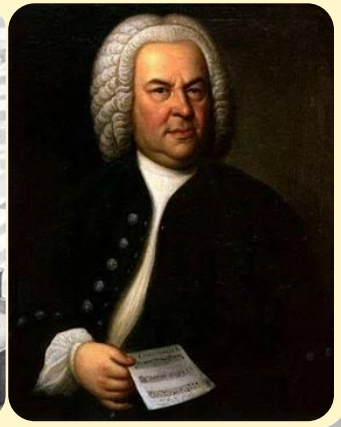


Einstein: my own work no longer mean much.
I come to the Institute merely to have the privilege to be able to walk home with Gödel

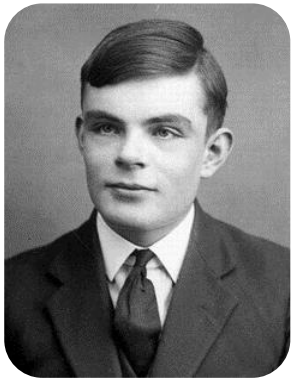
Gödel, Escher, Bach:
an Eternal Golden Braid

Douglas Hofstadter, 1979



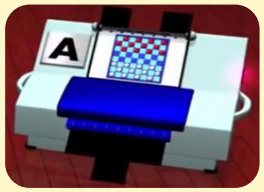


Alan Turing and Computation

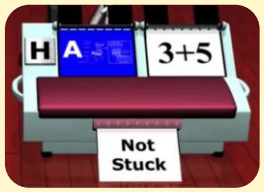


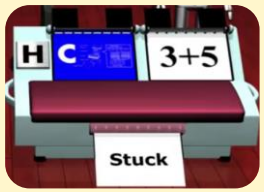
阿兰-图灵 Alan Turing (1912-1954)

- The founder of Computer Science and Artificial Intelligence
- Turing Machine describes what is computation
- Proved that Halting Problem for Turing machines is undecidable



Program **A** or **C** and an input, the program may "stuck" or not

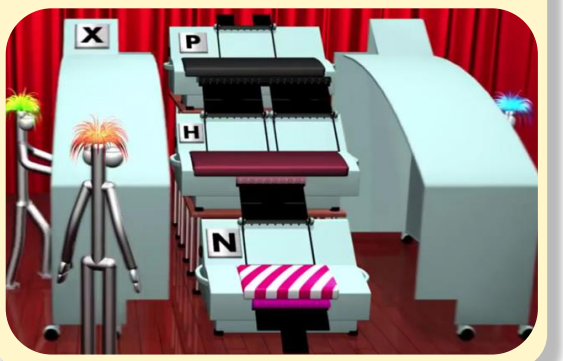




We hope to find a new program **H** to determine if **A** or **C** stuck

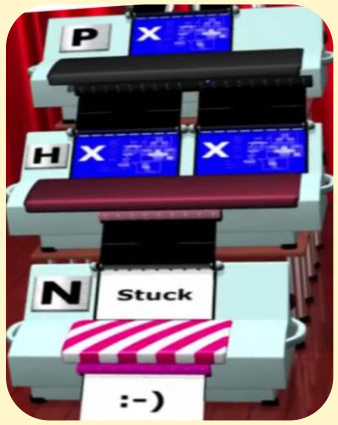
We build following new program **X** using machines **P**, **H**, **N**, where

- **P** is just a copy machine and
- **N** stuck if it receives "not stuck"



Program **H** does not exists!

- What if we put **X** into itself
- If **H** says this "stuck", then **N** makes it "not stuck"
- If **H** says this "not stuck", then **N** makes it "stuck",

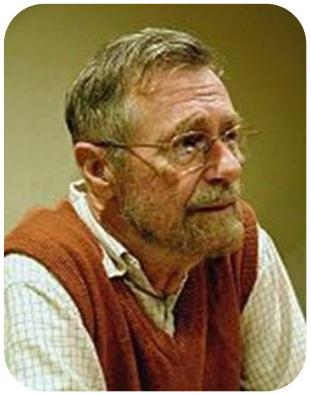


https://www.bilibili.com/video/BV1z441187ph?spm_id_from=333.999.0.0

A Road of Two Thousand Years

- It takes us more than 2000 years to build our math system correctly
- We finally realize that we can never really understand the real world!

Applications of Logics in EECS

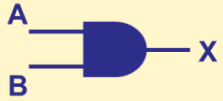


迪杰斯特拉 Edsger Dijkstra (1930-2002)

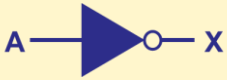
- One of the greatest computer scientists
- 搞了这么多年软件，错误不知犯了多少，现在觉悟了。我想，假如我早年在数理逻辑上好好下点功夫的话，我就不会犯这么多的错误，不少东西逻辑学家早就说了，可我不知道。要是我能年轻二十岁的话，就要回去学逻辑。

命题逻辑：数字电路设计

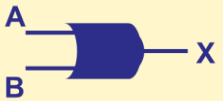
- 非门: X为1当且仅当A为0



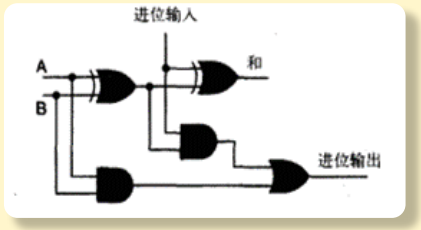
- 与门: X为1当且仅当A,B都为1



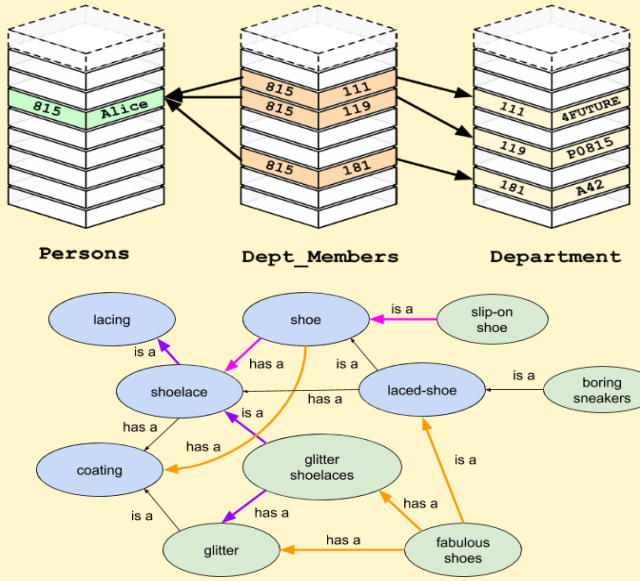
- 或门: X为1当且仅当A,B不全为0



- 二进制加法器

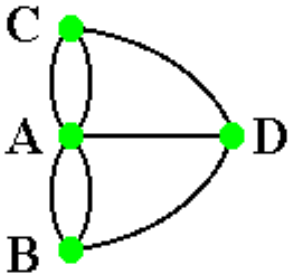


谓词逻辑：数据库、知识图谱



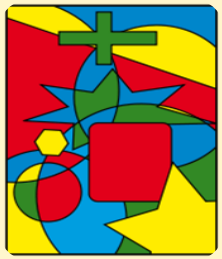
Graph Theory

- Graph theory is the study of graphs, which are mathematical structures used to model pairwise relations between objects
- A graph in this context is made up of vertices which are connected by edges.

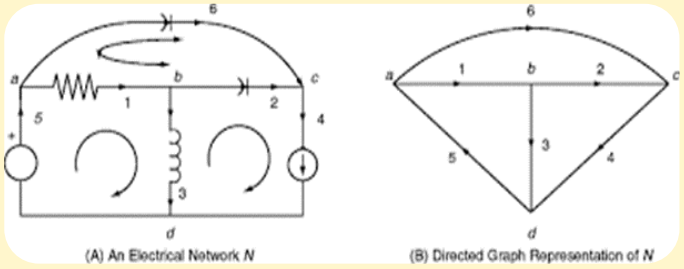


Euler solved the Seven Bridges of Königsberg (1736)

Four-Color Problem
proved in 1976 using computer

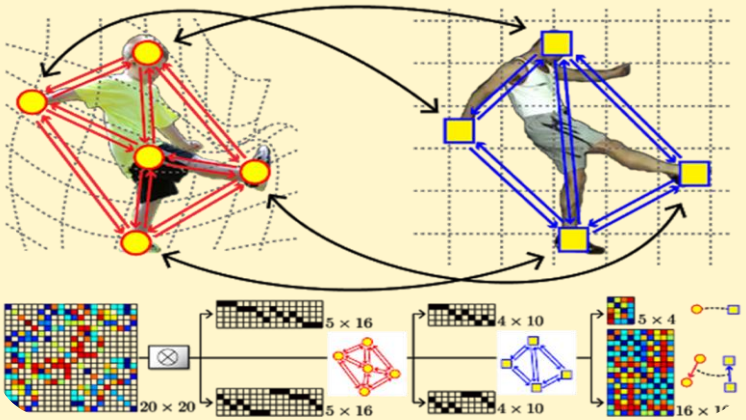


Kirchhoff studies electrical networks



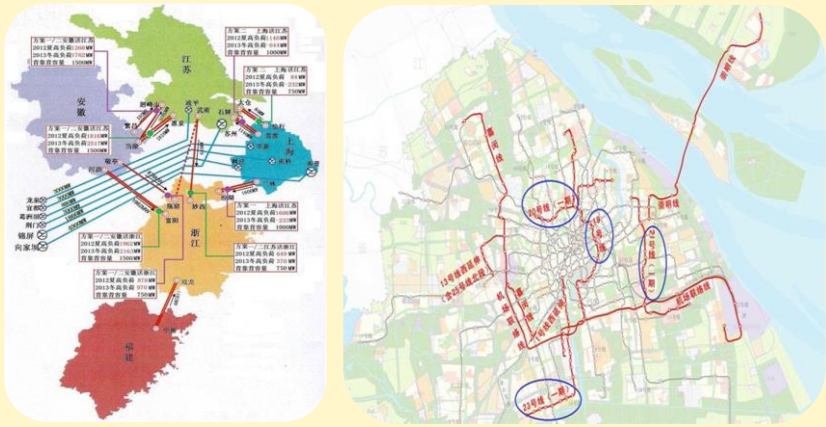
More Applications of Graph Theory

Graph Matching in Patten Recognition

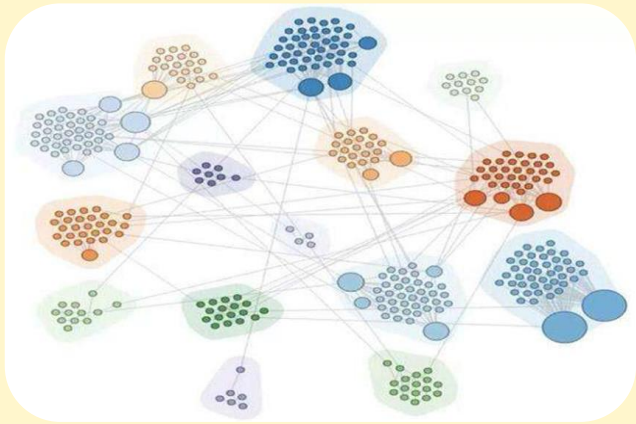


Shortest Path Search in Navigation

Network Flows in Power/Traffic Systems



Social Networks & Pandemic Spread



Back to Syllabus

Part I: Mathematical Logics (数理逻辑)---Week 1-6

- Propositional Logics (命题逻辑)
- Predicate Logics (谓词逻辑)
- Axiomatic Systems (公理系统)

Part II: Set Theory (集合论)---Week 7-12

- Naïve Set Theory (朴素集合论)
- Axiomatic Set Theory (公理集合论)
- Relations and Functions (关系与函数)

Part III: Graph Theory (图论)---Week 13-16

- Paths, Trees, Euler/Hamilton Graphs...

Thank You!