



网络空间安全基本原理

李琦

清华大学网研院



讨论



《三体》中有这样一个比喻：

一群原始人，每天都在琢磨怎么**提升弓箭的射程**，怎么在**箭尖上涂毒**，那么这群原始人基本上就完了
如果他们当中有一个不务正业的人，整天想着怎么能**升起一堆火**，研究**岩石或木头的构成**，那这群原始人距离发明火器就近了一步

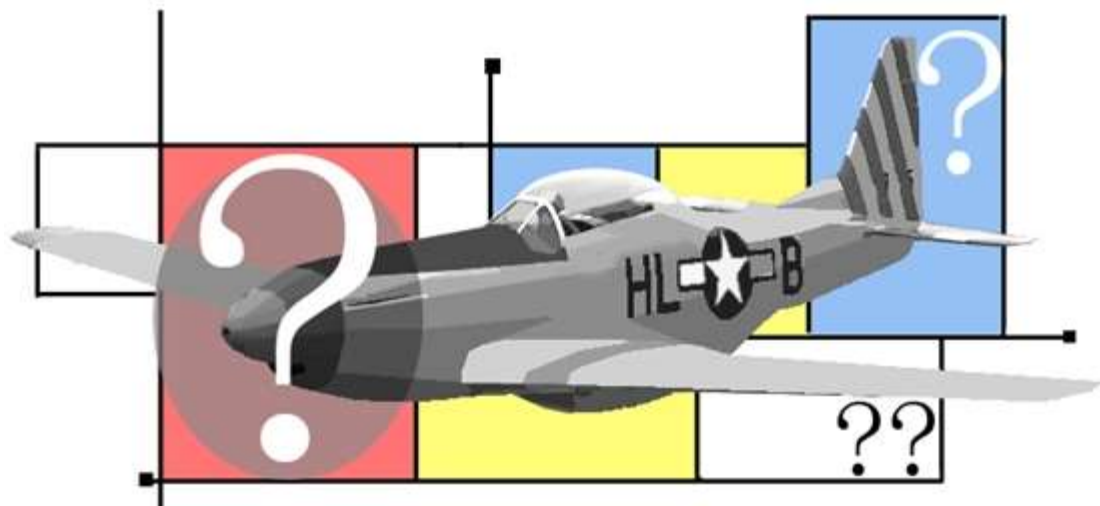
畅所欲言

对于这种说法你怎么看？



幸存者偏差

从某种意义上讲，第二次世界大战是飞机战的开端，谁抢到了制空权，谁就占据了主动。所以，战争期间，几乎每天都有大量飞机参战。于是问题就来了：敌人也不是吃干饭的，你派飞机过去，人家自然会反击，一来二去，飞机中弹、乃至失事，再正常不过，该怎么**提高飞机的生存率呢？**



考虑到防御与灵活性和持续作战的能力，军方想要为最需要的部位加装装甲，从而减小被击落的概率。
在哪里加装装甲，才能最大限度的保存飞机呢？



幸存者偏差

飞机部位	每平方英尺的平均弹孔数
引擎	1.11
机身	1.73
油料系统	1.55
其余部位	1.80



各部位被击中的概率应该是相等的，消失的弹孔在未能返航的飞机之上

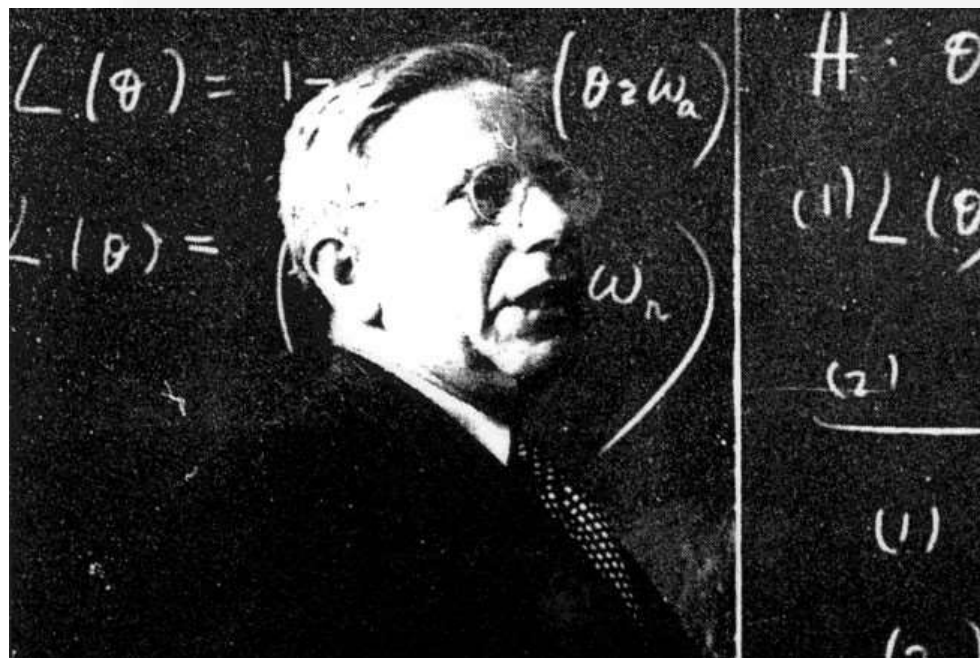


被击中概率最高的部位要给予重点防护，加装装甲，其余部位可以适量减少装甲



幸存者偏差

亚伯拉罕·瓦尔德(Abraham Wald), 1902年出生于罗马尼亚克鲁日, 由于出生于犹太世家, 他受教育的机会受到了某些限制, 只能靠自修弥补。瓦尔德先就读于克罗日大学, 1927年进入维也纳大学学习, 并在仅修了三门课之后拿到博士学位



二战前, 瓦尔德到达美国, 并在二战期间进入了**哥伦比亚大学统计研究小组**, 为美国军方服务

消失的弹孔与幸存者偏差



本章的内容组织



第一节 新的开始

- 畅想一个未来事件，提出五个亟待解决的实际问题



第二节 图论

- 图论的基础知识
- 回答开辟根据地的的问题



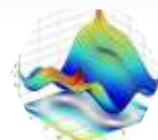
第三节 控制论

- 控制论的基础知识
- 回答获取策略集的问题



第六节 概率论与随机过程

- 概率论的基础知识
- 回答战略判断的问题



第五节 最优化理论

- 最优化理论的基础知识
- 回答资源规划的问题



第四节 博弈论

- 博弈论的基础知识
- 回答策略选择的问题



第1节 新的开始

- ✓ 如何开辟根据地?
- ✓ 如何设定策略集?
- ✓ 如何与敌人进行周旋?
- ✓ 如何充分利用我们的资源?
- ✓ 在什么地方拦截?



新的挑战



未来的某一天，世界科技空前发达，计算机技术也进化到了一定的高度，人们的生活已经**和计算机息息相关**



在一片祥和的景象中，突然迸出了不和谐的声音：一个前所未有的强大**计算机病毒**出现了，以难以阻挡的速度蔓延向世界的每一个角落



彼时，工厂停止运行、交通几乎瘫痪、经济基本处于停滞状态。**谁能成为新的救世主？**



面临的问题

战略准备 → 战略相持 → 战略反攻



如何的
“开辟地
属于”
自己



如何的
策略集
实施我
们



如何人
进行周
旋的？
敌



如何的
资源充
分利用
我



在截缓
什么，病
地能够毒
方极蔓
进行大延
拦延



已知的未知属于风险，风险可以用概率来表述，而未知的未知属于不确定性。

——弗兰克·奈特

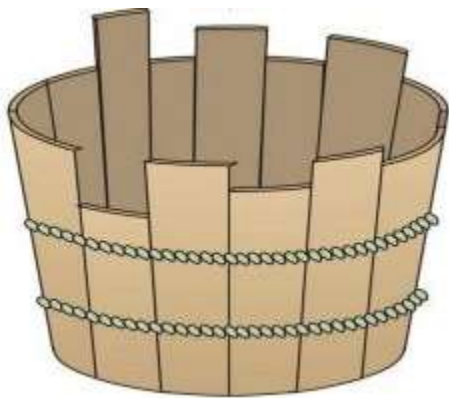
只有千日做贼，哪有千日防贼。

——清·《中国现在记》

- 硬件、软件都是一些复杂系统的集成，在理论和实践上是难以避免存在漏洞的
- 在经济全球化的大趋势下，后门的存在也是不可杜绝的
- 从网络防御者的角度，基于未知漏洞和后门的未知攻击，是未知的安全威胁，我们不知道从何处下手才能够实施有效的、有针对性的防御



网络安全的木桶原理



一只水桶能装多少水取决于它最短的那块木板。

——劳伦斯·彼得



- 你的系统有10个漏洞，黑客总是寻找最容易攻破的漏洞，这就是所谓的“安全木桶”上的**短板，最弱的一环**
- 无论你其他安全措施多么强大，黑客只要找到**一块短板**就行了

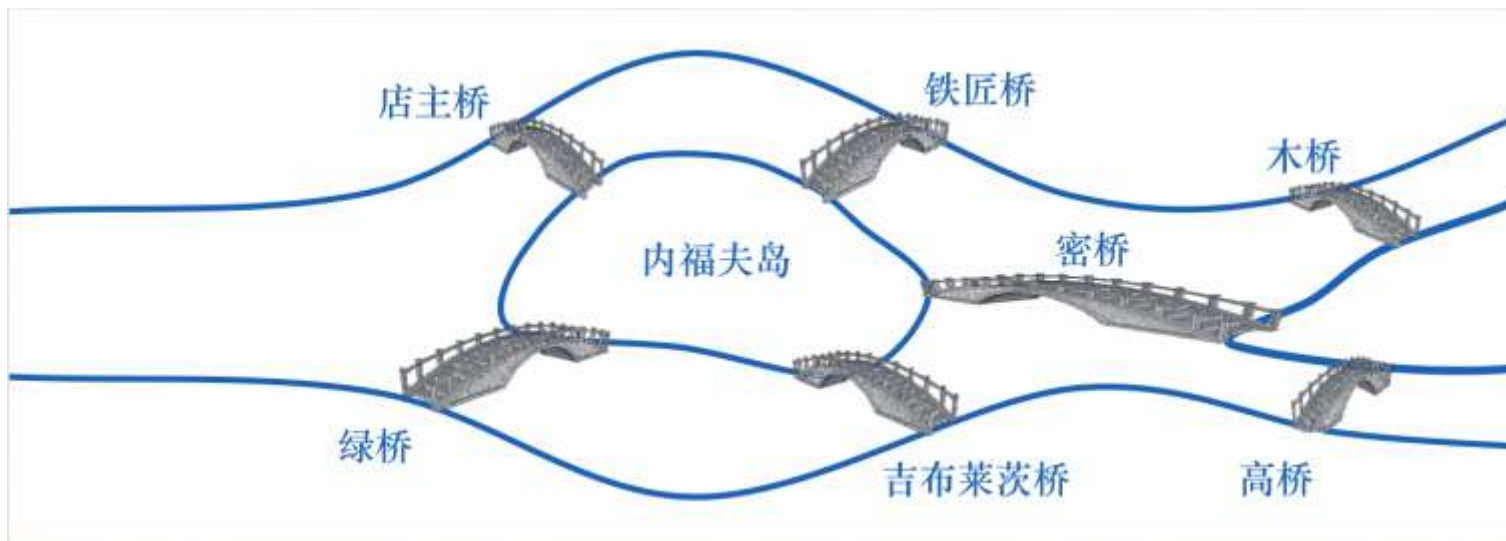


第2节 图论

- ✓ 起源
- ✓ 着色问题
- ✓ 网络结构与网络行为



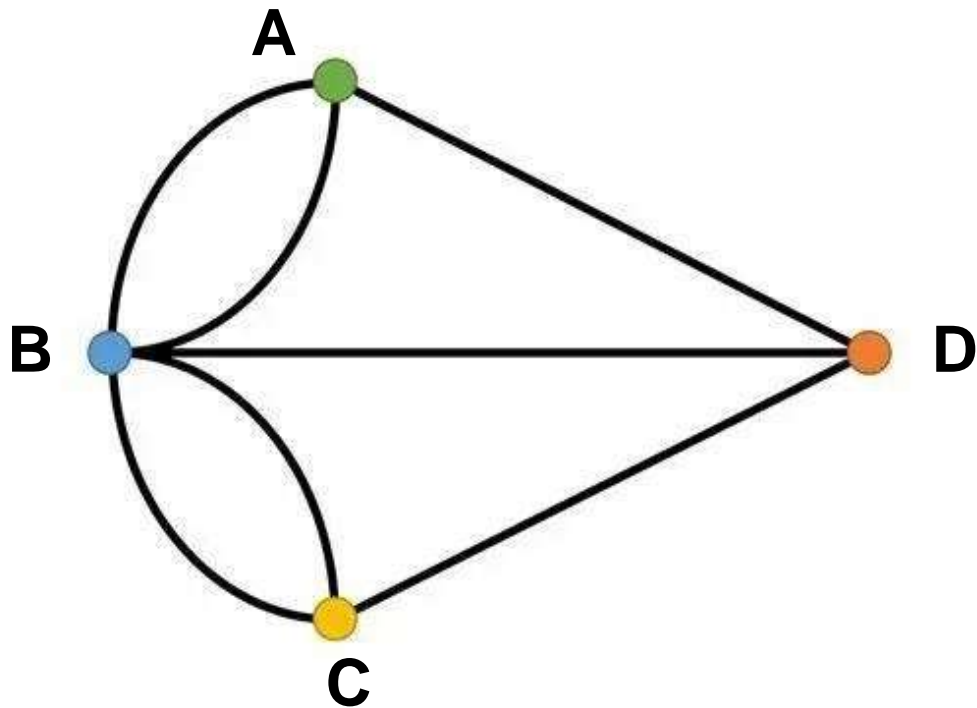
哥尼斯堡七桥问题



在18世纪，普鲁士哥尼斯堡有一条大河，河中有两个小岛。全城被大河分割成四块陆地，河上架有七座桥，把四块陆地联系了起来。当时许多市民都在思索一个问题：**一个散步者能否从某一陆地出发，不重复地经过每座桥一次，最后回到原来的出发地呢？**



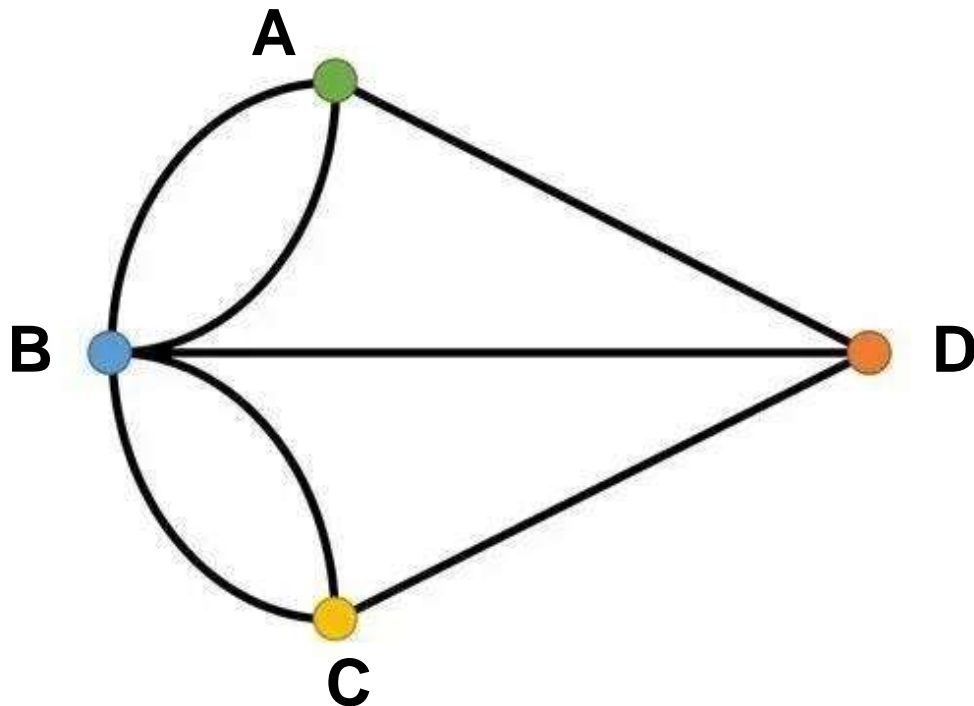
哥尼斯堡七桥问题



欧拉并没有去重复人们已失败了多次的试验，而是把七桥问题进行了**数学的抽象**。用A、B、C、D四个点表示四块陆地，用两点间的一条线表示连接两块陆地之间的一座桥，就得到如图所示的一个由四个点和七条线组成的图形



哥尼斯堡七桥问题



1736年，欧拉发表首篇关于图论的文章《关于位置几何问题的解法》
(*Solutio Problematis ad geometriam situs pertinentis*)，研究了哥尼斯堡
七桥问题，他也被称为图论之父

Google Scholar 1612



欧拉

- 瑞士数学家和物理学家。他被一些数学史学者称为历史上最伟大的两位数学家之一（另一位是卡尔·弗里德里克·高斯）
- 历史上最多产的数学家之一
 - 一生共写了886本书籍和论文
 - 彼得堡学院为了整理他的著作整整花了47年
- 人生波折：失明，火灾
 - 口述了几本书和400篇左右的论文
- 科学环境：普鲁士腓特烈大帝和俄国叶卡捷琳娜女皇慷慨地给了数学以无法报偿的资助
- 19世纪高斯：**“研究欧拉的著作永远是了解数学的最好方法”**



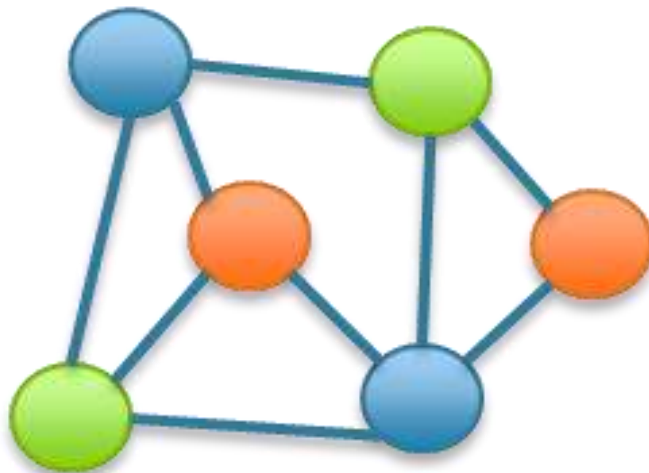
$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} a & b & d & c \\ b & c & a & d \\ c & d & b & a \\ d & a & c & b \end{bmatrix}$$

	6		5	9	3			
9		1				5		
	3		4				9	
1		8		2				4
4			3		9			1
2				1		6		9
	8				6		2	
		4				8		7
			7	8	5		1	



三色问题与交互式零知识证明

Alice (证明者)



Bob (验证者)

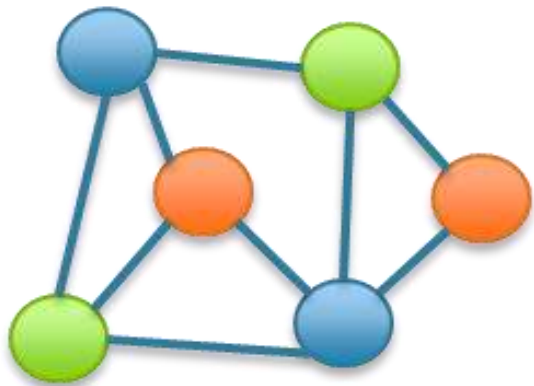


三色问题：一种NP完全问题

目的：**Alice试图证明她有三色问题的解，但不想把解告诉Bob**



三色问题与交互式零知识证明



Permute



Alice (证明者)



Bob (验证者)



1

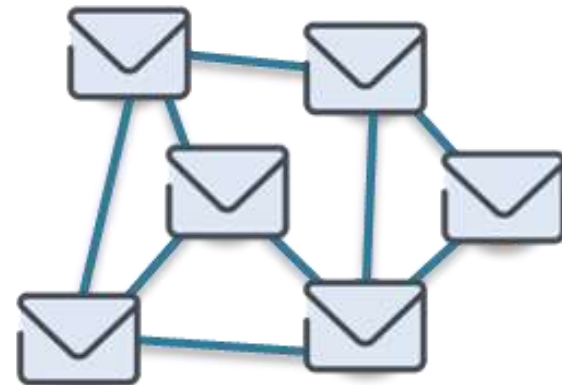
Commit

2

Pick 1 edge

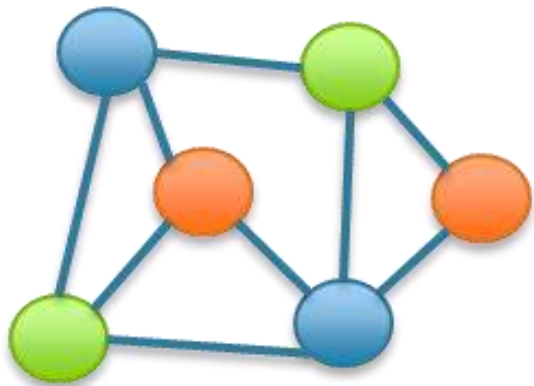
3

Open the nodes





三色问题与交互式零知识证明



Permute



Alice (证明者)



Bob (验证者)



1 Commit

2 Pick 1 edge

3 Open the nodes





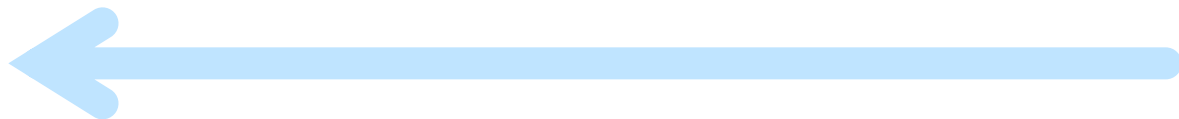
三色问题与交互式零知识证明

Alice (证明者)

Bob (验证者)



You do have the solution!



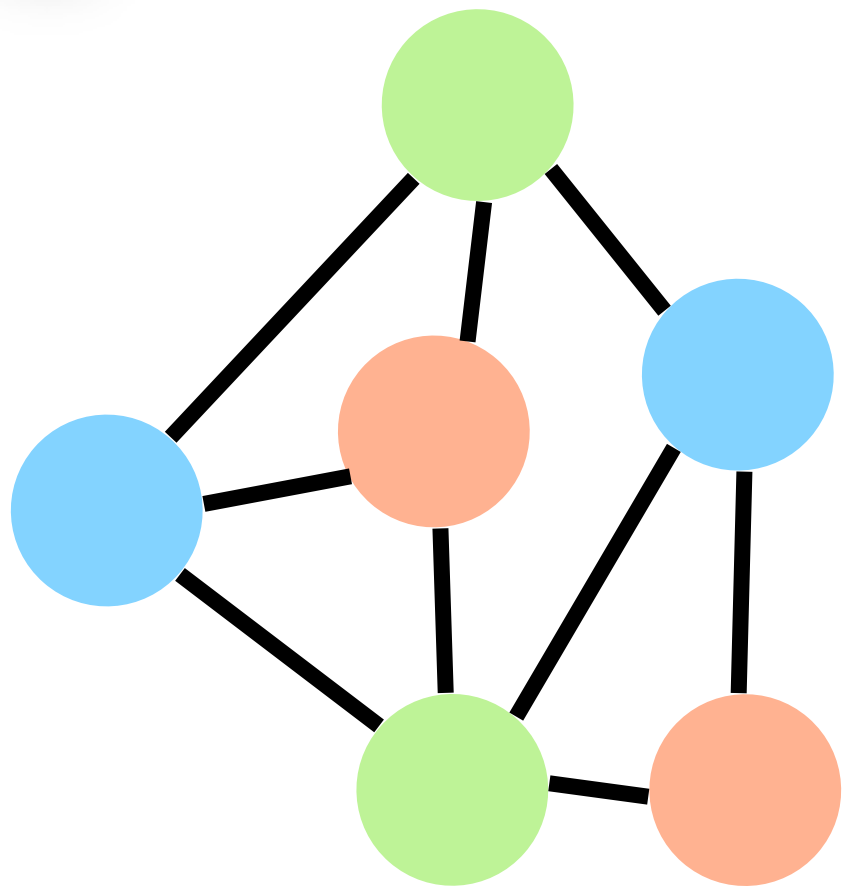
- After n round, the probability of Alice has a solution will be

$$Pr[\cdot] = 1 - \frac{1}{|E|^n}$$

- If n is very large, Alice will convince Bob



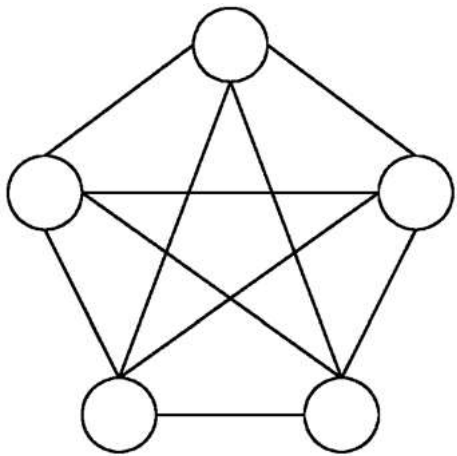
图的定义



- 图论中所研究的图，并不是几何学中的图形，而是客观世界中某些事物联系的一个**数学抽象**
- 如左图所示，一般用顶点代表事物，用边表示事物间的关系
- 这种由顶点及边所组成的图就是图论中所研究的图，一般用**G**表示

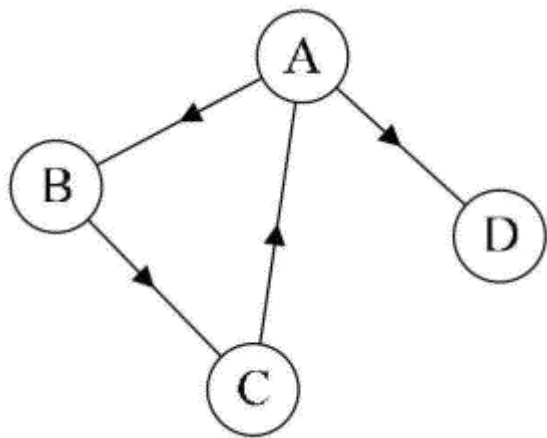


两个重要定理



- 定理1:

设图G中有E条边，V个顶点，则G中所有顶点的度数之和为边数的两倍，即 $\sum D(V) = 2 * E$



- 定理2:

图G中度为奇数的顶点个数恰有偶数个



地图染色问题

对任意一幅地图的每个区域进行着色，使得相邻的区域不同色。**问最少需要多少种颜色才能实现？**



Hint: 每个地图可以导出一个图，用顶点表示国家，相应的边表示国家相邻



四色猜想

四色猜想现在应该叫做**四色定理**。四色定理的本质是**二维平面的固有属性**，即平面内不可出现交叉而没有公共点的两条直线。二维平面内无法构造五个或五个以上两两相连区域



- 1976年，伊利诺斯大学的两台电子计算机，用1200个小时，100亿个判断，最终证明了四色定理。**但有很多人认为计算机证明无法给出令人信服的思考过程**

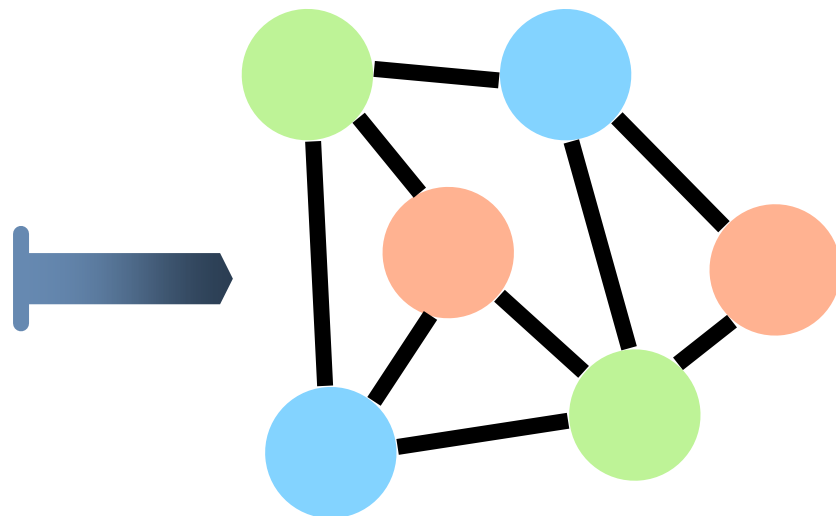
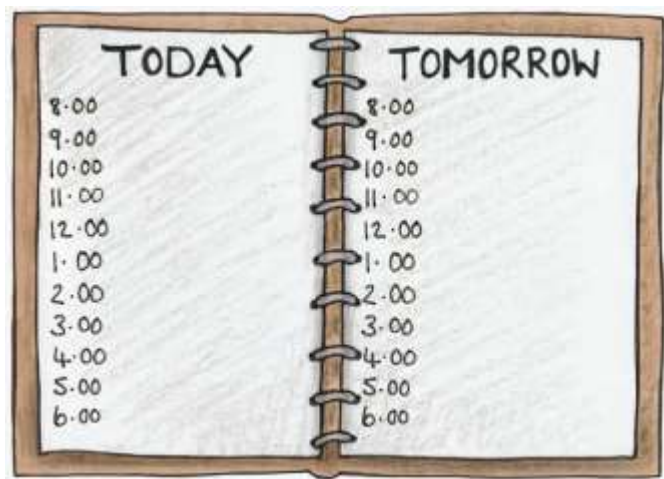


着色问题的应用

许多由图论表述的现实问题都需要把节点集或者边集划分为一些不相交的子集，使得同一子集中的所有元素互不相邻，这些问题都可以**形式化为相应的着色问题**来进行分析：

例如：

- 会议安排
- 考试日程设置
- 化学品存放



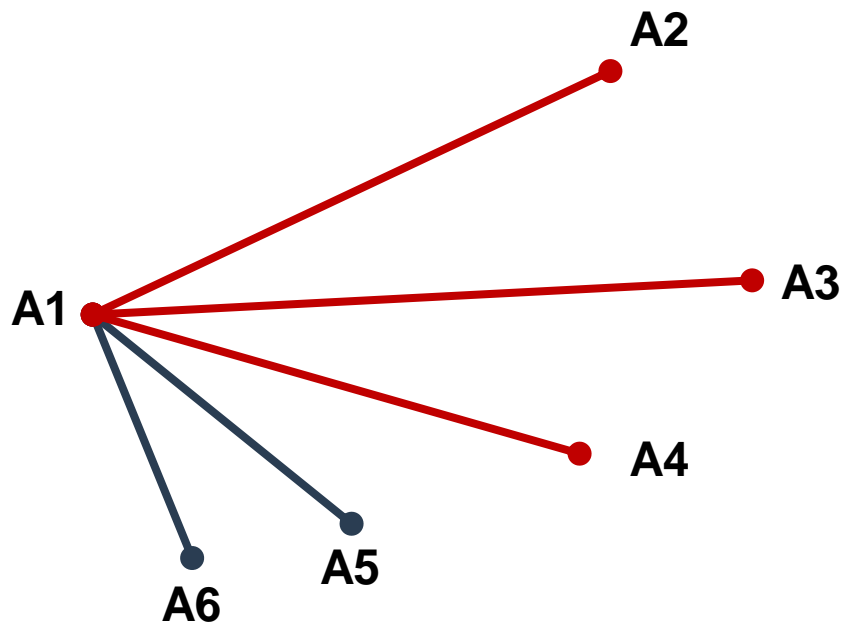


Ramsey问题

证明题：

任意6个人中，一定存在3个人相互认识，或者3个人相互都不认识

等价于证明6个顶点的完全图的边，用红、蓝二色任意着色，必然至少存在一个红色边三角形，或蓝色边三角形



- Ramsey数 $R(p,q)$ ：代表了红蓝染色一个完全图，图中至少包含一个红色 K_p 或者蓝色 K_q 的完全图的最少边数
- 目前只有10个Ramsey数的值被确定，其他的都还是未知的
- 美国数学会前任主席R.L.Graham曾说过，要确定Ramsey数 $R(5, 5)$ 在100年之内是不可能的



网络结构对传播的影响——级联行为

- 场景
 - 一个社会网络；A，B两类事物要在其中流行
 - B是“旧的”，一直以来大家都采用B
 - A是“新的”，开始吸引了几个坚定份子
- 假设
 - 每个人只能采纳A或B之一
 - 两个相邻的人若都采用A，则得回报a；若都采用B，则得回报b；若采用不一样的，则回报0
 - 在从一种选择换到另一种过程中没有其他成本
 - **同时采用A和B，带来哪些不同？**

选择A或者B?



选择A或者B?

- 在一条边上的博弈
 - 如果v和w都选择A，它们分别得到回报 $a > 0$
 - 如果它们都选择B，分别得到回报 $b > 0$
 - 如果它们选择不同的选项，那么都得到回报为0
- **协调博弈**：一个节点v需要考虑其所有邻居选择的综合结果后再做决策

表达为一个博弈

节点V \ 节点W	A	B
A	a, a	$0, 0$
B	$0, 0$	b, b



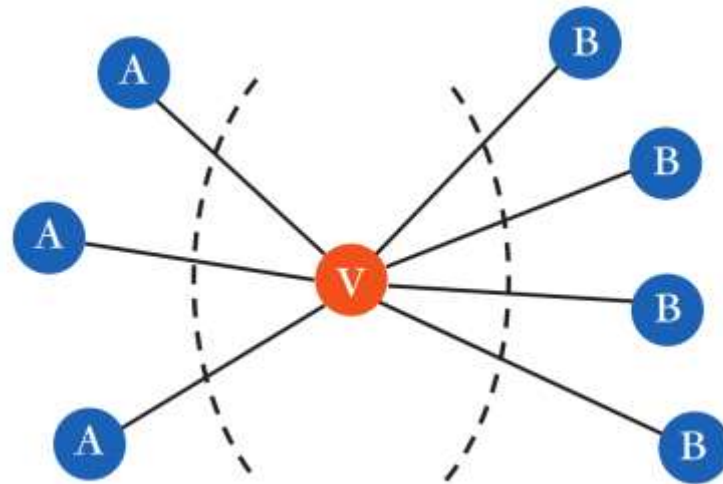
网络节点的决策门槛

- 设 v 有 d 个邻居，在某一时刻，若占比 p 的邻居选A，占比 $1-p$ 的邻居选B
- v 选A的回报： pda
选B回报： $(1-p)db$
- 如果 $pda \geq (1-p)db$ ，即若 $p \geq b/(a+b)$ ，则选A好；
否则，选B更好

博弈存在两个极端的情形，也是两个明显的均衡

- 所有节点都选择了A
- 所有节点都选择了B
(互为最佳应对，没人有动机改变)

有 $(1-p)d$ 邻居用B



有 pd 邻居用A

门槛

$$\frac{b}{a+b} = q$$

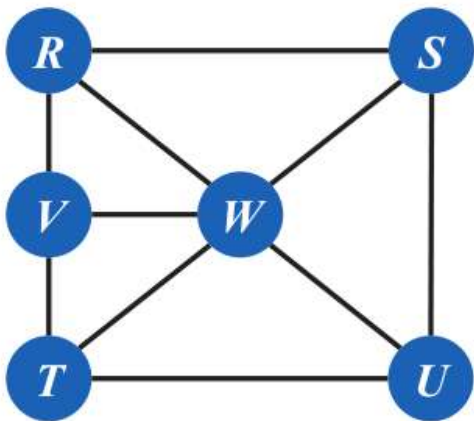


新生事物在网络中的传播过程

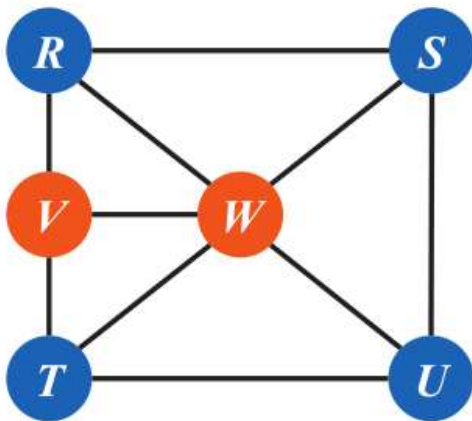
- 同时考察每一个采用B的节点的邻居采用A的比例是否达到门槛 $q=b/(a+b)$
 - 是，则节点放弃B，转用A；否则继续采用B
- 重复这过程，直到网络中采用A的节点集合不再变化

例： $a=3$ ； $b=2$ ； $q=2/5$

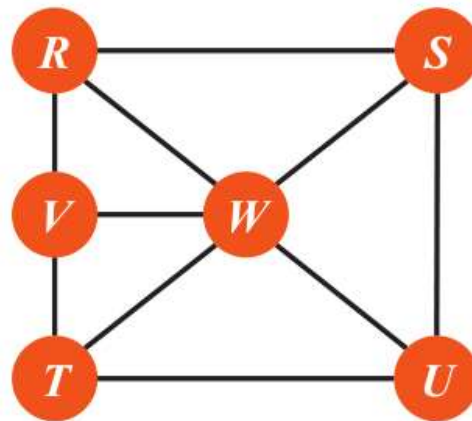
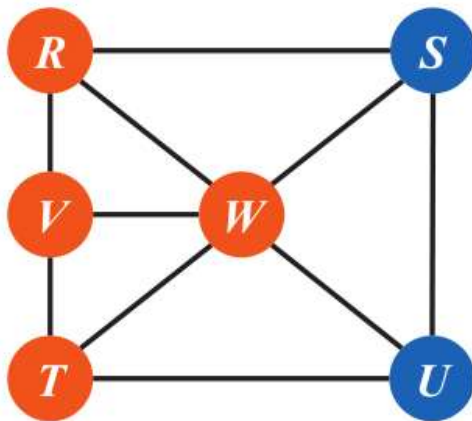
经过两步，实现完全级联



基本网络



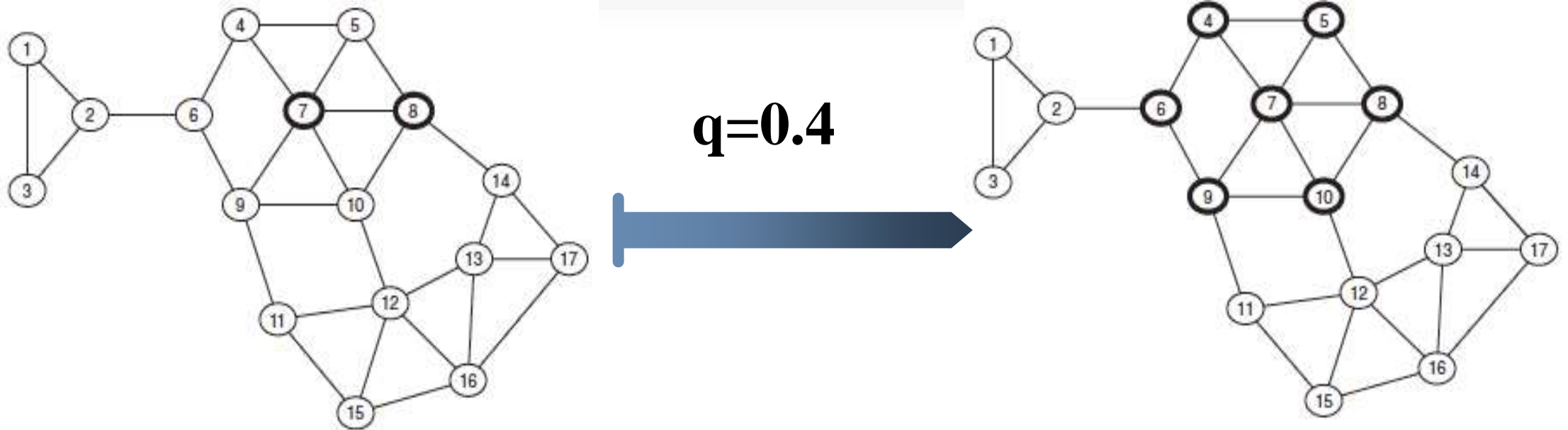
假设V和W最初采用A





一个不能形成完全级联的例子

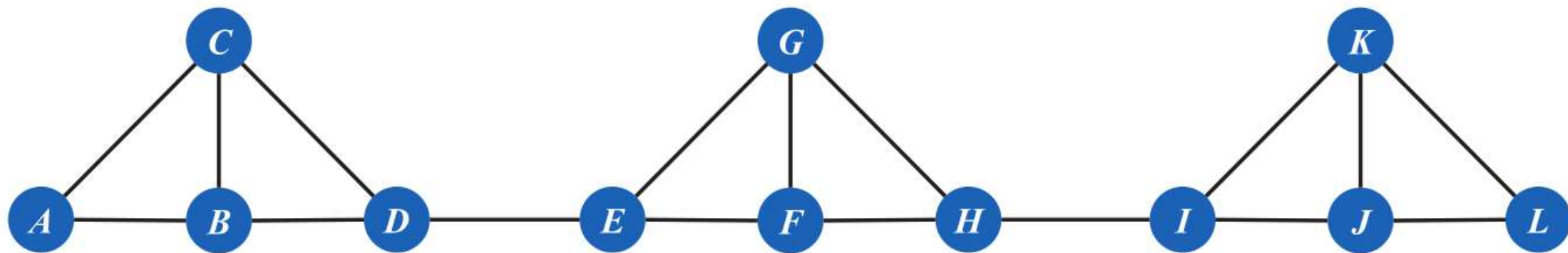
- $a=3$, $b=2$, $q=2/5$
- 最初, 7、8是A的初用节点, 其他所有节点均采用B; 传播一步后, 5、10加入A节点集合; 两步后, 4, 9加入; 三步后, 6加入。
- 随后, 级联停止, 采用A的群体不再扩大





刻画阻挡级联的因素——聚簇

- 聚簇（“抱团”）：称一个节点集合为密度为 r 的聚簇，若其中每个节点至少有占比为 r 的网络邻居也属于这个节点集合
- 下图有3个密度为 $2/3$ 的聚簇



剩余网络中包含一个
密度大于 $1-q$ 的聚簇

充要条件



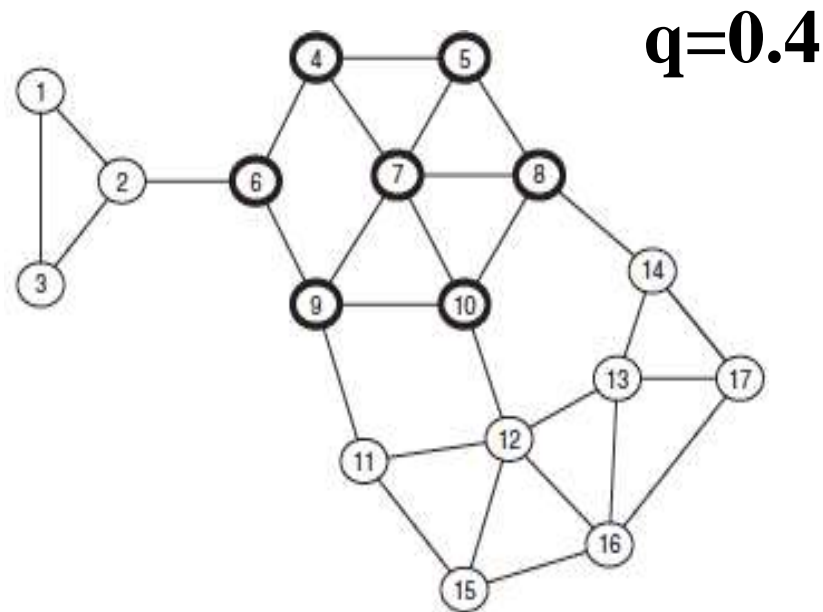
初用节点集不能形成
A的完全级联



蠕虫病毒的传播

再看网络级联

- 大多数蠕虫病毒的传播需要载体，通过类似电子邮件、网页链接、P2P连接等方式向外扩展
- 这种传播方式与新事物在社交网络传播有着非常类似的性质



那么蠕虫病毒如何突破聚簇的阻碍，形成病毒A的完全级联传播？

- **方法一：提高 A 的吸引力**，从而减少 q 值，如 q 减至 $1/5$ ，A 可以形成完全级联
- **方法二：**在密度大于 $1-q$ 的聚簇中选择**关键节点**，利用其他外部因素使其感染A，致使A在这些区域得以扩散



如何开辟属于自己的“领地”

战略准备 → 战略相持 → 战略反攻



如何的
开辟“
领地
于”
自？



如何策
何略
实施集
我？
们



如何进
和行
我们周
旋的？
敌



如何的
充资源
利？
用我



在截缓
什，病
么能毒
地够的
方极蔓
进大延
行地？
拦延

- 对于“网络人”来说，工作、战场都在网络之上，因而我们不同的“网络人”要进行协作必须要有一个健康的网络作为支撑
- 开辟根据地的实质就是寻找擅长不同领域安全问题的红、白帽子集合与对应的边界节点集合之间的一个“最优”匹配



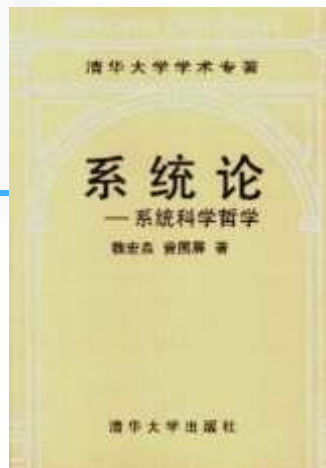
第3节 控制论

- ✓ 可能性空间
- ✓ 随机控制
- ✓ 有记忆控制
- ✓ 共轭控制
- ✓ 负反馈调节



“三论”

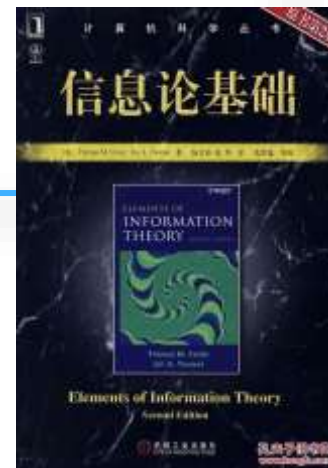
20 世纪 40 年代



提出系统概念并揭示其一般规律



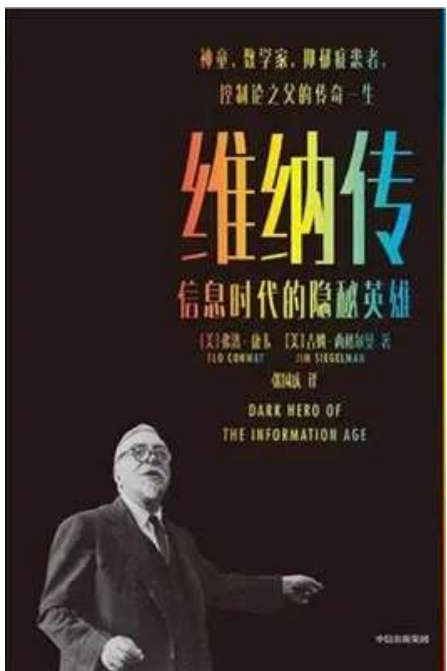
研究系统演变过程中的规律性



研究控制的实现过程



控制论的起源



维纳 N.Wiener(1894-1964)

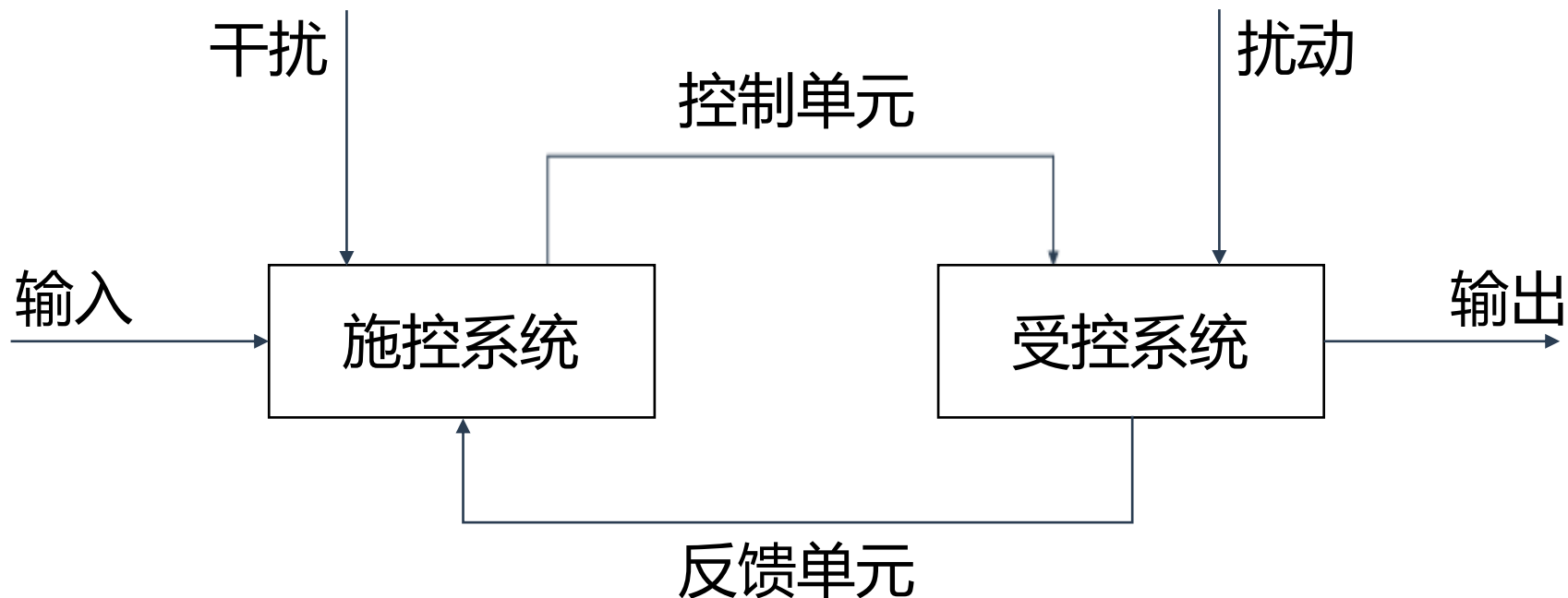
- 美国数学家，3岁就能读写
- 11岁上大学，学数学，但喜爱物理、无线电、生物和哲学
- 14岁考进哈佛大学研究生院学动物学后又去学哲学
- 18岁获得了哈佛大学数理逻辑博士学位



1948年10月，维纳写出划时代著作《控制论》，标志着一门新学科的诞生



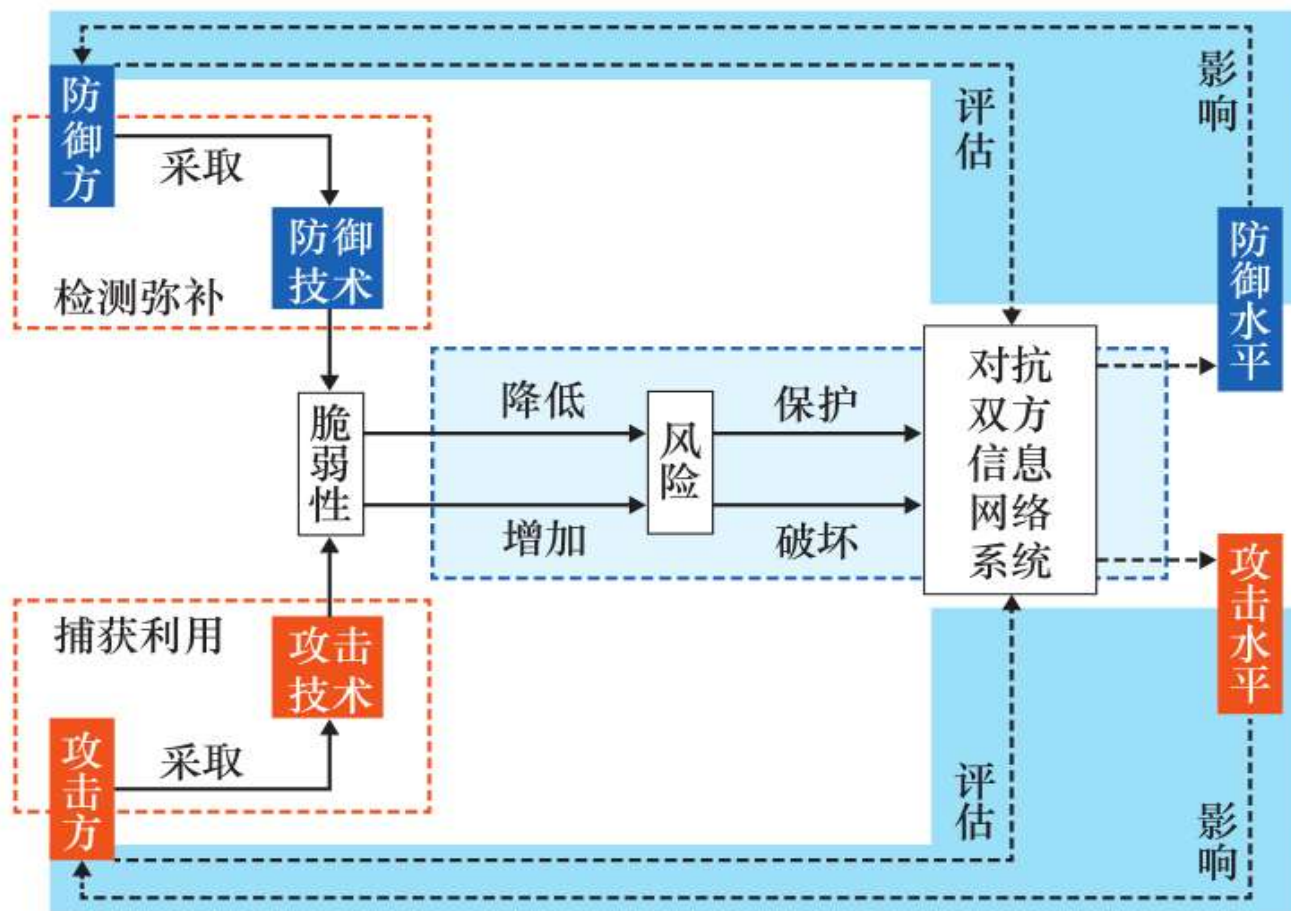
网络攻防控制模型



- 网络控制系统是典型的人机系统，由离散的事件驱动，并由离散事件按照一定运行规则相互作用来导致**状态演化**的动态系统
- 施控者可以作用与受控者，受控者也可以反作用于施控者。前者叫做控制，后者叫做反馈



网络攻防控制中的反馈模型



信息特别是与网络系统相关的攻防知识是网络攻防控制的核心

网络攻防控制就是网络攻防双方通过控制相关的网络攻防知识并根据做出决策的反馈来不断靠近目标的过程



《控制论》(Cybernetics)



控制论的基本理论观点：

机器与生物一般都是通过负反馈来达到控制的目的

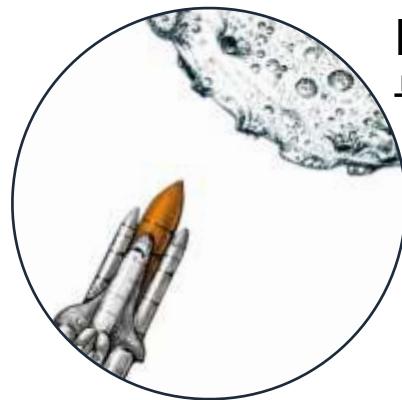
维纳把反馈的概念推广到一切控制系统，把反馈理解为从受控对象的输出中**提取一部分信息作为下一步的输入**，从而对再输出发生影响的过程



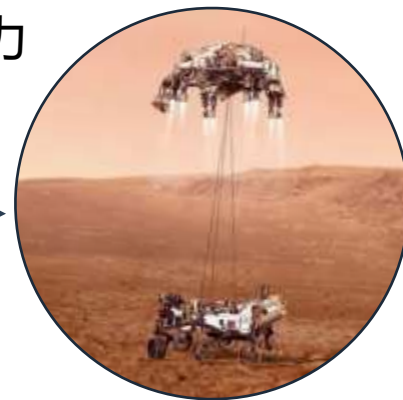
负反馈调节

选择一：精确的瞄准，在发射之前按照计算好的提前量瞄准发射

选择二：在发射的过程中不断调整自己的飞行方向

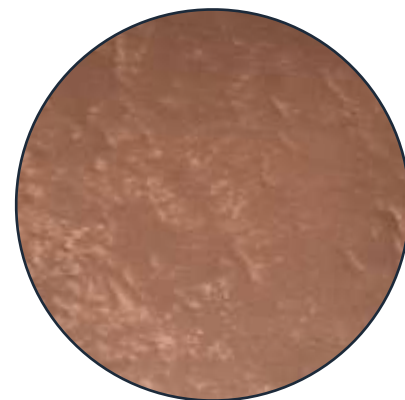


2020年7月30日，NASA发射了毅力号火星探测器



2021年2月19日，毅力号火星车成功登陆到火星的杰泽罗陨石坑内

毅力号火星车传回登陆画面

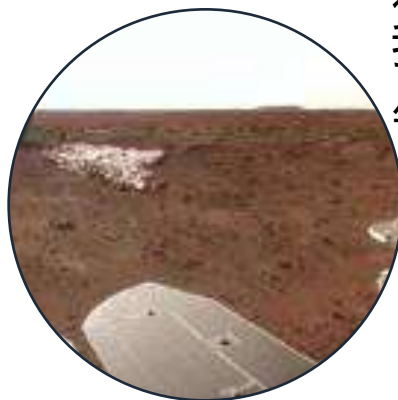


2021年2月10日，**天问一号**探测器抵达火星轨道，成为我国第一颗人造火星卫星



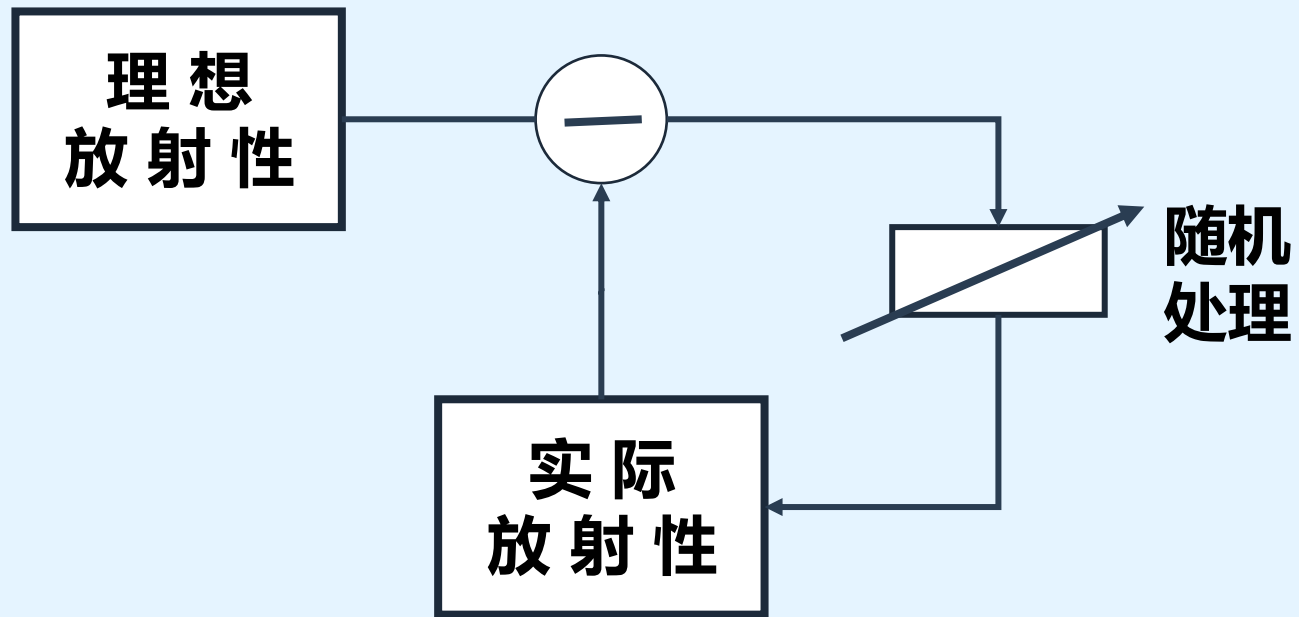
中国

5月22日10时40分，**祝融号**火星探测车**登陆火星**，开启了探测之旅





负反馈调节

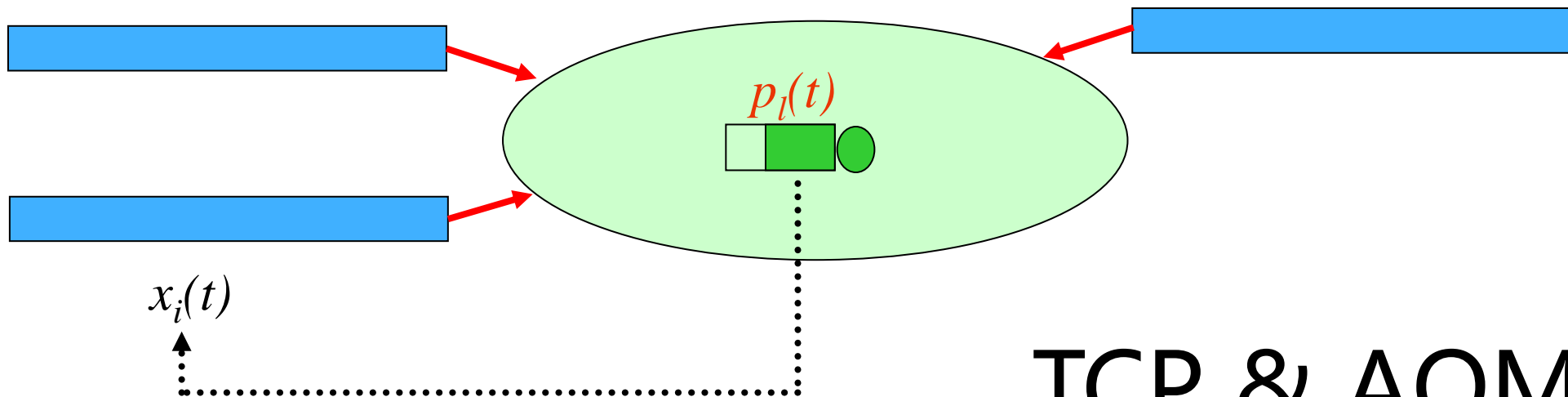


当人们一次的控制能力**不足以达到目标**时，通过收集到的信息，不断调整控制方案，直到达到目标的过程。其中，负反馈调节一定要有两个环节：

- 系统一旦出现目标差，便自动出现某种减少目标差的反应
- 减少目标差的调节一次一次地发挥作用，使得对目标地逼近进行积累



网络中的反馈调节——拥塞控制



TCP & AQM

拥塞控制信号 $p_l(t)$		
	反馈信号 $p_l(t)$	代表算法
1	Loss	DropTail
2	Queue length	RED
3	Queueing delay	Vegas, BBR
4	Price	REM

本质是通过不同**信号的反馈**，调整自身的应对策略，使得网络向着目标状态演化的过程



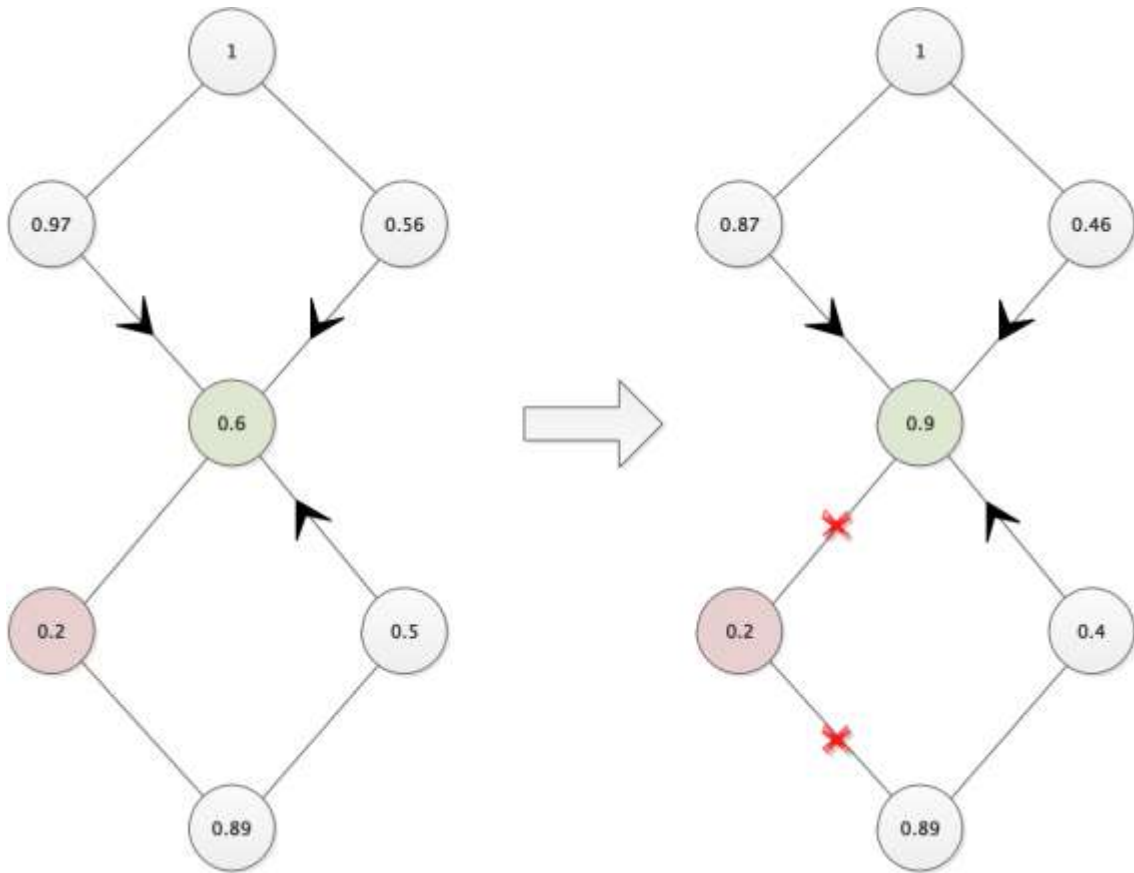
网络中的行为度分析

核心思想

通过对相关节点的观察和量化分析，
获取节点信息反馈，并差异化的控制
节点交互能力

意义

- 连接“真实性”与“安全性”
- 细化对节点可信、可靠程度的反馈，
增加反馈的信息量
- 为网络态势和安全提供支撑





细化的反馈信息——行为度量

分类：直接偏离度、间接偏离度、推荐节点偏离度

直接偏离度

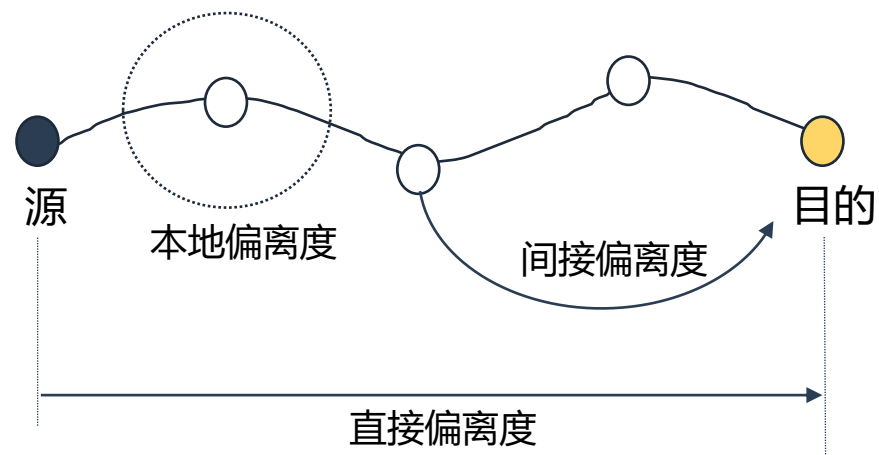
源端依据交互历史对目的端计算出的偏离度数值，按时间片更新，用以描述源端对目的端的直接评价

间接偏离度

转发路径上依据一定规则选取的推荐节点，针对目的节点给出的综合偏离度值，用以描述本次通信中相关节点对目的端的评价

推荐节点偏离度

根据与推荐节点直接相连的周边节点，对推荐节点的偏离度评价，计算得到的推荐节点自身偏离度，用以描述推荐节点本身的可靠性



通过引入偏离度，将节点信息映射目标由简单的离散二元空间转化为 $[0,1]$ 连续实数空间，增强了反馈信息的容纳能力，从而**提升了反馈控制能力**



如何实施我们的策略集

战略准备 → 战略相持 → 战略反攻



如己的
何的开
辟领
属地
于“
自？



如的
何策
实略
施集
我？
们



如人
何进
和我
周旋
的？
敌



如的
何资
充源
分利？
用我



在截缓
什，病
么能毒
地够的
方极蔓
进大延
行地？
拦延

- 在对“敌人”一无所知的时候，我们可以进行**随机接触**，随便挑选一种应对策略来应对对方
- 根据不同的反馈，逐步调整应对策略，最终找到一些行之有效的策略集合



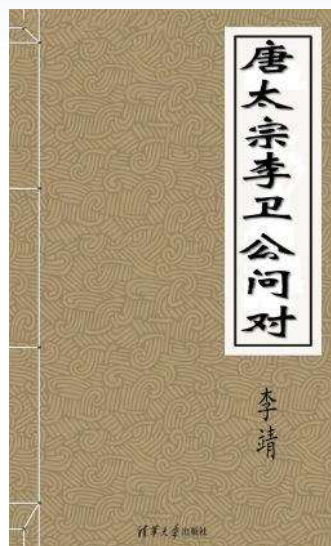
第4节 博弈论

- ✓ 非合作博弈
- ✓ 合作博弈
- ✓ 纳什讨价还价



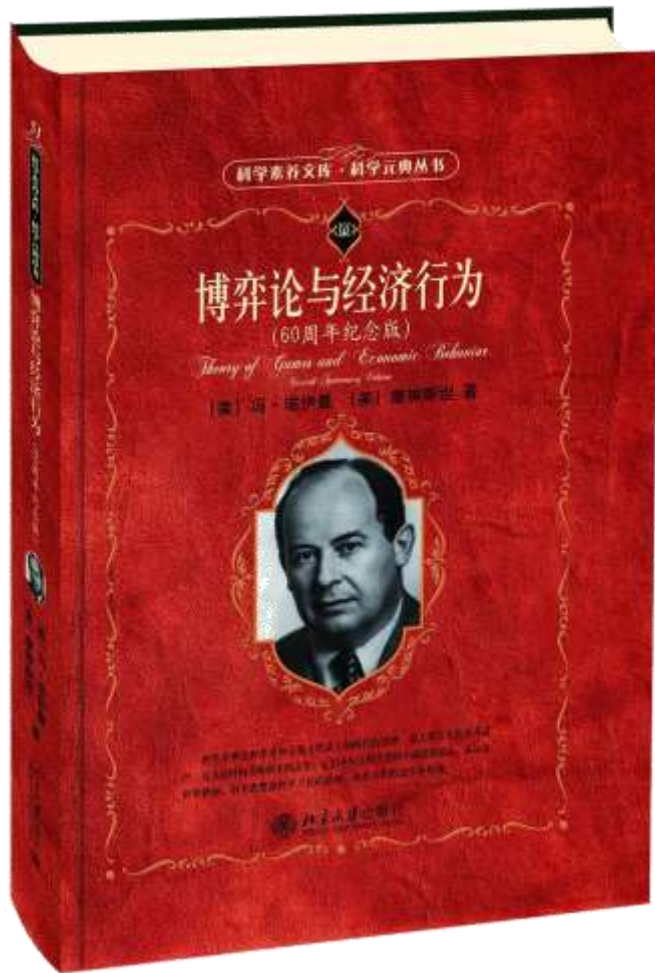
博弈论的起源

博弈论的历史可以追溯到很久之前的古人，是人们在不断地实践中总结出来地实践经验和古老的智慧





博弈论的起源



冯·诺伊曼 (1903-1957)



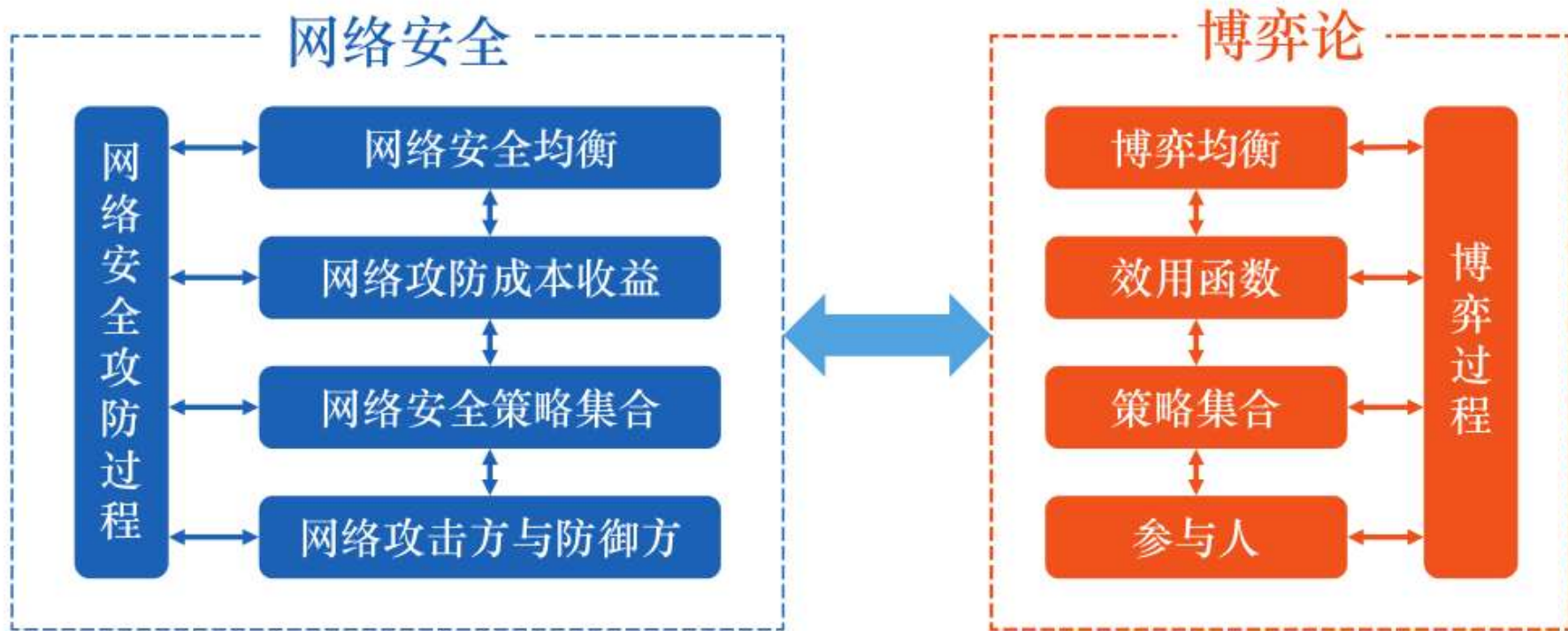
摩根斯坦 (1902-1977)

1944年出版的《博弈论和经济行为》标志着

博弈论作为一门学科**登上了历史舞台**



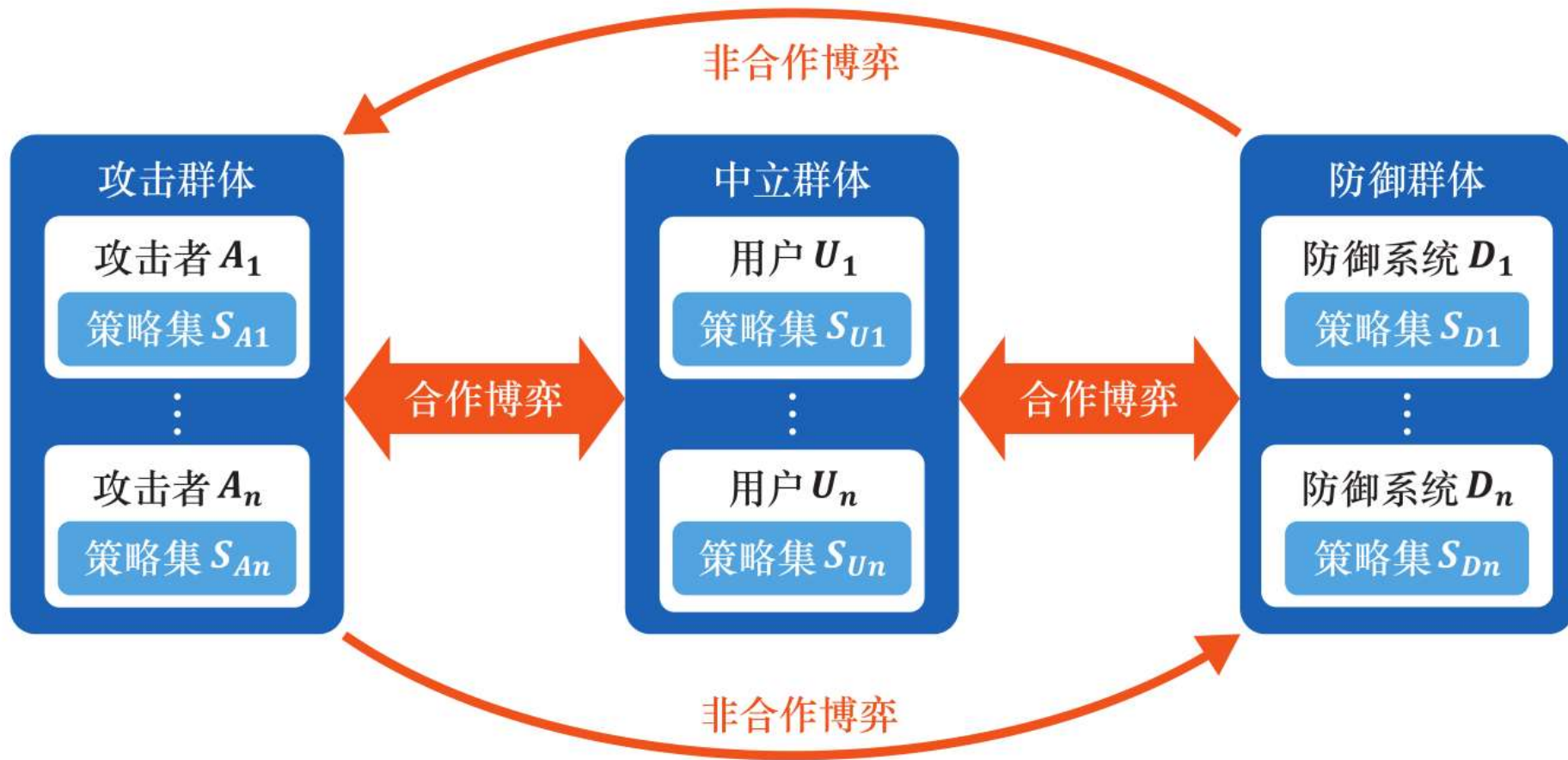
网络安全中的博弈论



网络安全的要素、特征与博弈论的元素、特征具有一致性和符合性。攻击者和防御者之间的对抗行为符合博弈论思想，而博弈论提供了一个解决网络安全分析和建模的**数学框架**，有助于理解攻防矛盾冲突、预测攻击行为和选取最优防御策略，因此将博弈论思想应用于网络安全问题研究具有较好的**合理性和可行性**



网络安全中的博弈论



网络安全态势博弈模型 NSG (Network Situation Game)



博弈论

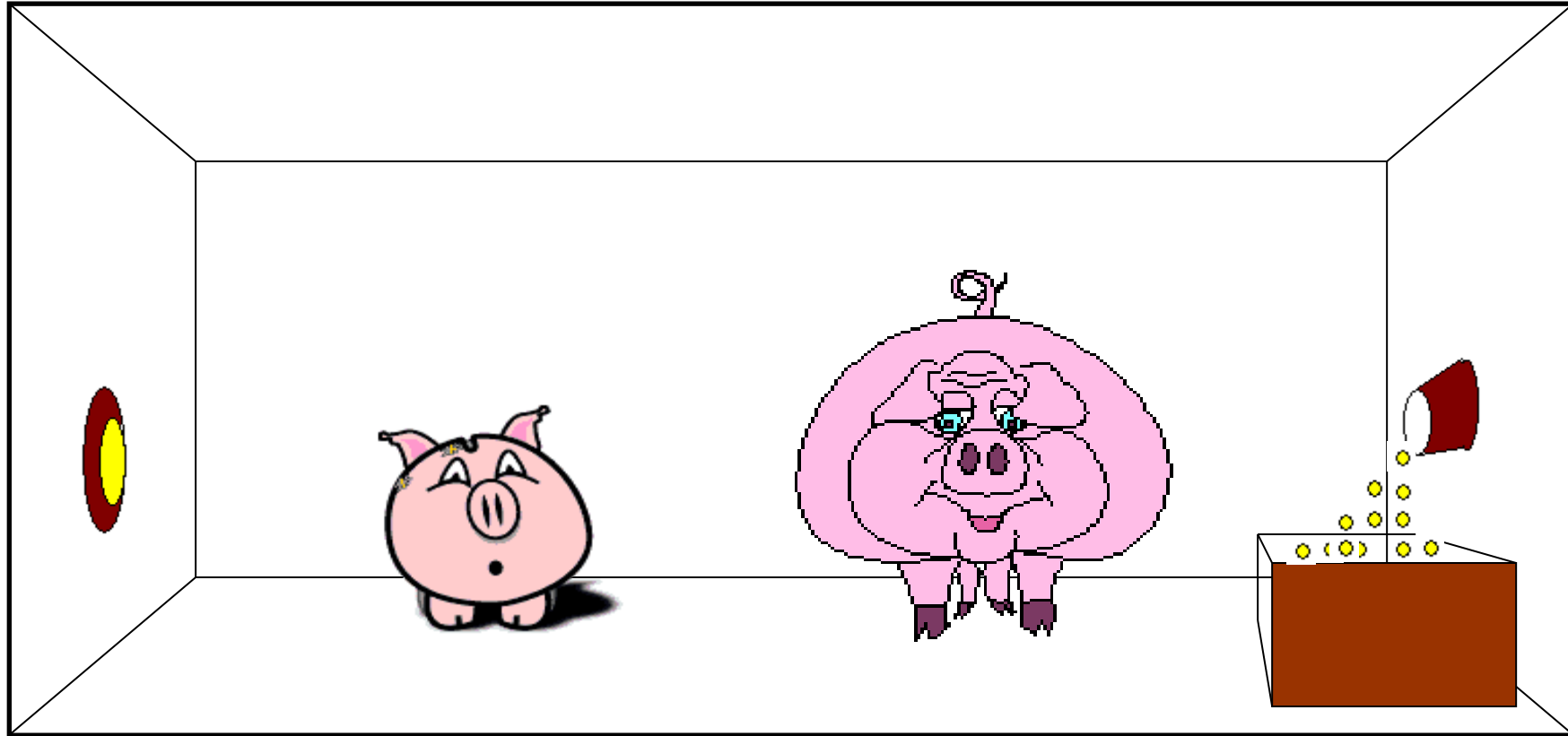
博弈论 (Game Theory)

- 研究**互动的博弈**中参与者各自的选择策略
- 研究**机智而理性**的决策者之间的冲突及合作
- 参与者必须意识到他们的决策是相互影响的

博弈论把这些复杂关系**理论化**，以便分析其中的逻辑和规律，并对实际决策提供指导或借鉴



智猪博弈



**Cost to press
button = 2 units**

**When button is pressed,
food given = 10 units**



智猪博弈

Decisions, decisions...



Big Pig



Little Pig

	Press	Wait
Press	5 , 1	4 , 4
Wait	9 , -1	0 , 0



什么是一个博弈

- 博弈有下列要素
 - 至少**两个** 参与者
 - 每个参与者的**策略**
 - (策略) 集合
 - 博弈结果的优先关系





什么是一个博弈

参与者

- 一般概念
- 个人，公司，国家，协议实体

策略 (Strategy)

- 给定信息集下，一个策略决定了在每一个时间点上参与者选择何种行动
- 是参与者行动计划的一个完整描述，告诉参与者在每一种可预见的情况下选择什么行动

结果 (Outcome)

- 由每个参与者的策略组合确定

支付 (Payoff, 收益)

- 结果到效用的函数

优先关系

- 通过针对结果的效用（收益）函数来评价



合作与非合作

Robert Aumann

- 与Thomas Schelling分享了2005年诺贝尔经济学奖
- “合作和非合作方法不应当被看作在分析不同类型的博弈，相反，它们是看待同一个博弈的不同方式”



以色列经济学家

通过博弈论分析
改进了我们对冲突
和合作的理解



非合作博弈

- 第一个被深入研究的博弈
- 参与者的利益完全对立
 - 一方的收益就是另一方的损失
 - 可以用一项来表示博弈矩阵
- 直观的求解思路
 - 参与者最大化自己的收益
 - 期望得到唯一解

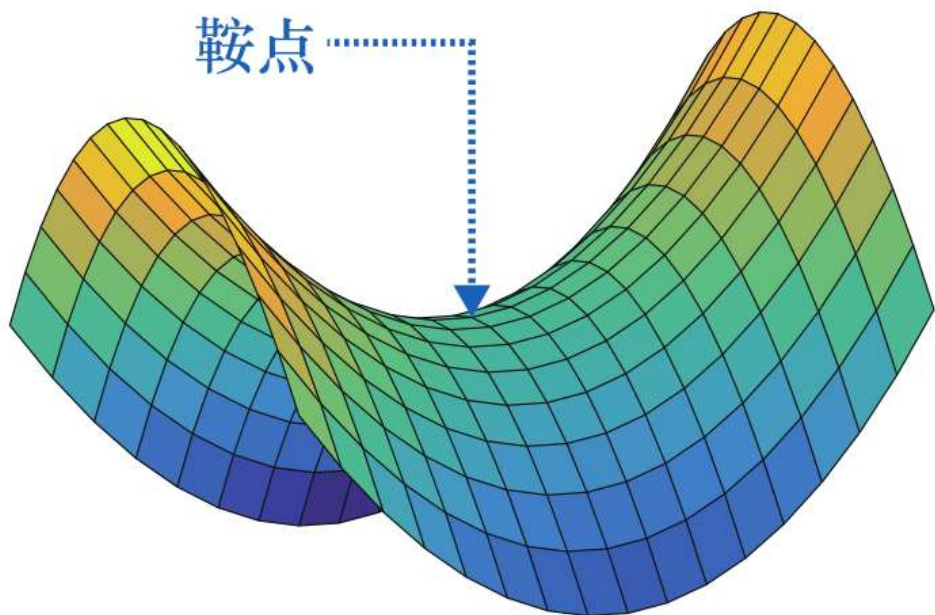


两人零和博弈



博弈的求解

寻找收益矩阵中的鞍点

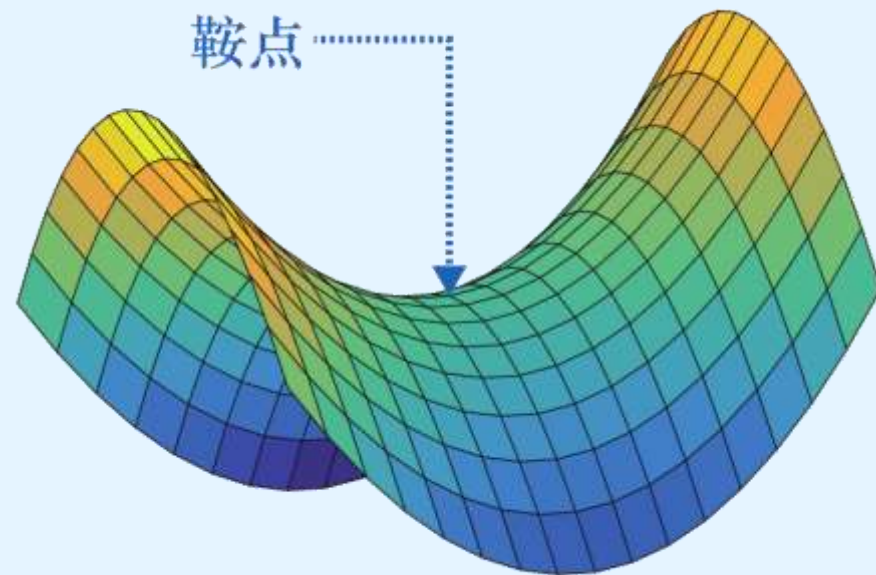


- 一个结果是鞍点，如果它是
 - **行中最小值、列中最大值**
- 鞍点原理
 - 参与人应该选择博弈中的鞍点
- 博弈的值
 - 如果鞍点存在，就是鞍点的值



博弈的求解

		参与人2		
		A	B	D
参与人1	A	12	-1	0
	C	5	2	3
	D	-16	0	-1



- 为什么参与人1相信参与人2会选择B?
 - 选择B能够保证**参与人2最多损失** v (这里是2)
- 为什么参与人2相信参与人1会选择C?
 - 选择C能保证**参与人1最少获得** v (这里是2)

这是为什么选择鞍点的合理原因！



混合策略

- 参与人为他的策略集关联概率分布
 - 参与人可以决定如何选择分布
- 按照**数学期望**计算收益

		参与人2	
		1/3	2/3
参与人1	A	4	0
	B	-5	3



参与人1选择A时的收益 = $(1/3)*4 + (2/3)*0 = 4/3$

参与人1选择B时的收益 = $(1/3)*(-5) + (2/3)*3 = 1/3$

**应该如何决定
概率分布？**



混合策略

- 参与人为他的策略集关联概率分布
 - 参与人可以决定如何选择分布
- 按照**数学期望**计算收益

		参与者2	
		x	1-x
参与者1	A	4	0
	B	-5	3

参与者1选择A时的收益 = $x*4 + (1-x)*0 = 4x$

参与者1选择B时的收益 = $x*(-5) + (1-x)*3 = 3-8x$



$$4x = 3 - 8x,$$

$$\text{Thus } x = 1/4$$

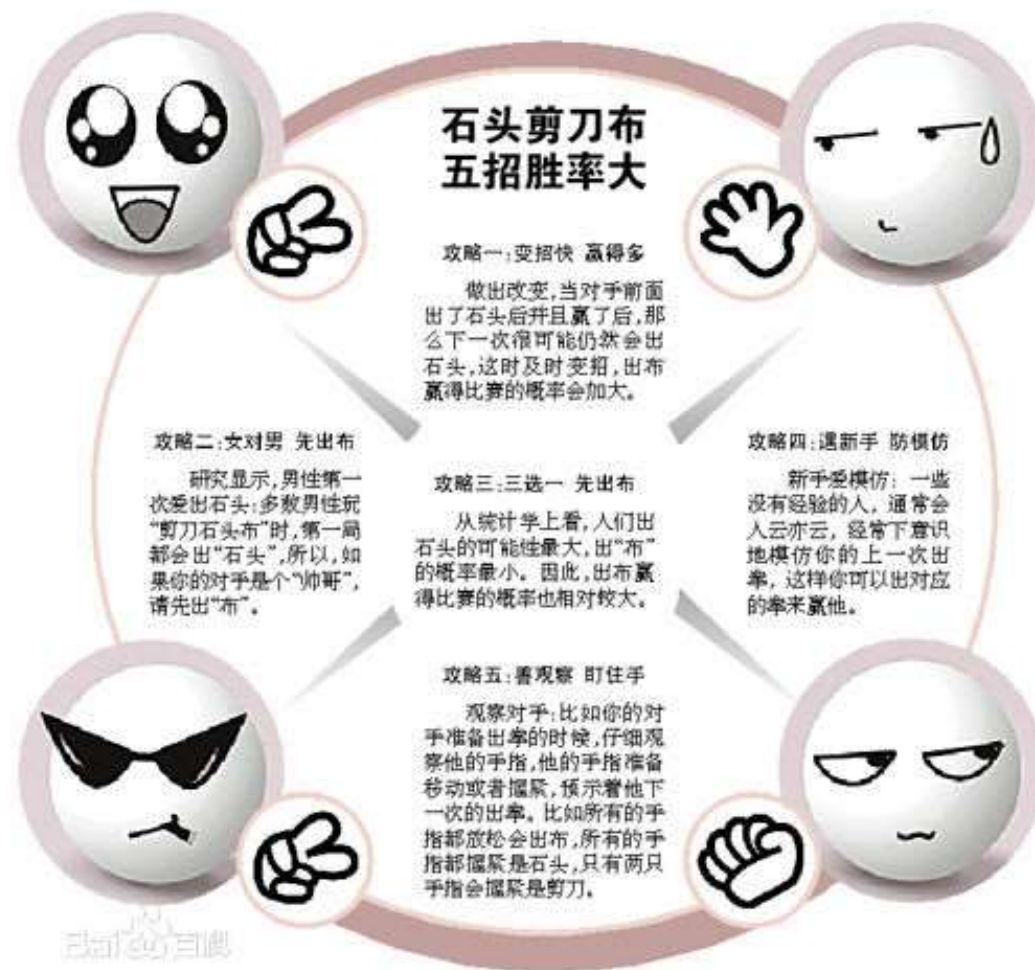


混合策略



参与人的最优混合策略应该是

石头 $1/3$ 剪刀 $1/3$ 布 $1/3$





极小极大定理

任何一个两人**零和**博弈都有一个混合策略的解（有时候是纯策略），
解的收益是博弈的值

- $\text{Max-min} = v = \text{Min-max}$
- v 是唯一的
- 纯策略情况下可能存在多个均衡
- 完全可以互换



1928冯·诺依曼给出了证明，标志着博弈论的诞生



纳什均衡

- 每个两人博弈都存在至少一个纯策略或者混合策略均衡
- 1950年纳什采用不动点定理进行了证明
- 获得1994年**诺贝尔经济学奖**（海萨尼，泽尔腾）
 - 在非合作博弈的均衡分析理论方面做出了开创贡献，对博弈论和经济学产生了重大影响



只要其它参与者不变换策略选择，任何**单个参与者不可能单方面通过变换策略来提高收益**



囚徒困境

- 著名的博弈实例
 - 1950年提出
- 两名嫌疑犯因为共同犯罪被逮捕
 - **隔离审讯**，可以选择承认罪行（confess）或者保持沉默（silent）

		Suspect 2	
		S	C
Suspect 1	S	2, 2	10, 1
	C	1, 10	5, 5

Payoff is years in jail
(smaller is better)

Better outcome

Single NEP



合作博弈

面对博弈，往往首先考虑**合作**，合作无法达成，则进行非合作博弈



合作的三种情况

- 事先可以达成有约束力的承诺，直接使用合作博弈方法
- 事先无法达成有约束力的承诺，使用能实现合作结果的非合作方法，如讨价还价博弈（Nash Bargaining）
- 无限次重复博弈，如无限次囚徒困境，仍然有可能达成合作解



合作博弈

- 一个**联盟**是参与人集合的子集，他们之间采取合作策略，并且就如何**分配收益**达成一致
- P 是参与人集合，共有 N 个参与人

- 联盟用大写字母 S, T, U 表示
- 给定一个联盟 $S \subseteq P$ ，它的对手联盟则是

$$S^c = P - S = \{p \in P : p \notin S\}$$





合作博弈

Strategy	Payoff vectors
(1,1,1)	(-2, 1, 2)
(1,1,2)	(1, 1,-1)
(1,2,1)	(0,-1, 2)
(1,2,2)	(-1, 2, 0)
(2,1,1)	(1,-1, 1)
(2,1,2)	(0, 0, 1)
(2,2,1)	(1, 0, 0)
(2,2,2)	(1, 2,-2)

Table1: Consider a 3-player game

- 这个博弈中, $P = \{P1, P2, P3\}$
- 共有8个联盟:
 - 3 个单一参与人: $\{P1\}, \{P2\}, \{P3\}$
 - 3 个两参与人: $\{P1, P2\}, \{P1, P3\}, \{P2, P3\}$
 - 大联盟: P 本身
 - 空联盟: \emptyset
- 一般来说, N 个参与人的博弈, 共有 2^N 个联盟



合作博弈

- 考虑一个联盟 $S = \{P_1, P_3\}$, 则 $S^c = \{P_2\}$
- 联盟 S 有四个纯联合策略: $\{(1, 1), (1, 2), (2, 1), (2, 2)\}$. 对于 S^c , 策略是1或者2, 则矩阵如下:

	1	2
(1,1)	(0, 1)	(2,-1)
(1,2)	(0, 1)	(-1, 2)
(2,1)	(2,-1)	(1, 0)
(2,2)	(1, 0)	(-1, 2)

联盟的最大值称为 S 的特征函数, 用 $v(S)$ 表示, S 的成员可以保证至少获得 $v(S)$ 的收益



合作博弈的解

功利主义：Shapley值

- 功利主义 (utilitarianism) , 即效益主义, 提倡追求 “最大幸福” (Maximum Happiness)
- 主要代表人物约翰·斯图亚特·密尔 (John Stuart Mill)、杰瑞米·边沁 (Jeremy Bentham) 等

平均主义：核

- 核中任意一个分配都不会导致参与者组合脱离总合作。如果核中包含一个解 x , 那么参与者不会形成其他联盟来代替



Shapley值

- 由 **L.S. Shapley** 于 1953 年提出，以一种公平的方式定义了一种分配，计算了每一位参与者的最终收益“应该”是多少
- 考虑了参与者对其所在联盟的边际效益
- 如果博弈的特征函数是 v ，参与者 p_i 所属联盟为 S ，那么

$$\delta(p_i, S) = v(S) - v(S - \{p_i\})$$

即为衡量该参与者对联盟的贡献大小（**称为
边际贡献**）





纳什讨价还价(Nash Bargaining)

John F. Nash, Jr. The Bargaining Problem.
Econometrica, Vol. 18, No. 2 (Apr., 1950), pp.
155-162, **Google 引用超过10000**



两人讨价还价场景：

- 两人合作的总收益大于各自单干的收益之和
- 两人需要一个规则来分配合作后获得的“蛋糕”，每人都以自己的收益最大为目标，因此存在一个“讨价还价”的过程
- 如果两人达成协议，则按照协议分配收益；否则，只能单干，获取较少收益



纳什讨价还价(Nash Bargaining)

公理1：个体理性

- 合作后每个人的收益都不少于单干时的收益，即

$$\varphi_1(F, v) \geq v_1, \quad \varphi_2(F, v) \geq v_2$$

公理3：对称性

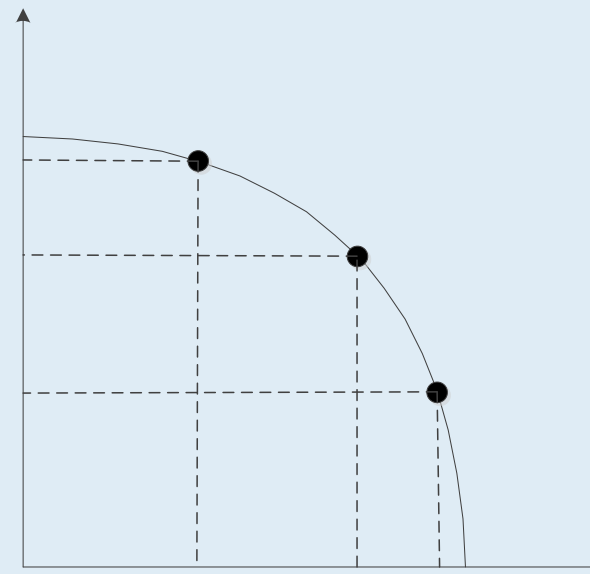
- 参与人的收益配置互换后也是可行的，地位相同的人待遇也相同，即：

如果 $(x_1, x_2) \in F$ ，必有 $(x_2, x_1) \in F$

如果 $v_1 = v_2$ ，那么 $\varphi_1(F, v) = \varphi_2(F, v)$

公理2：Pareto强有效

- 纳什讨价还价解必定位于Pareto边界上





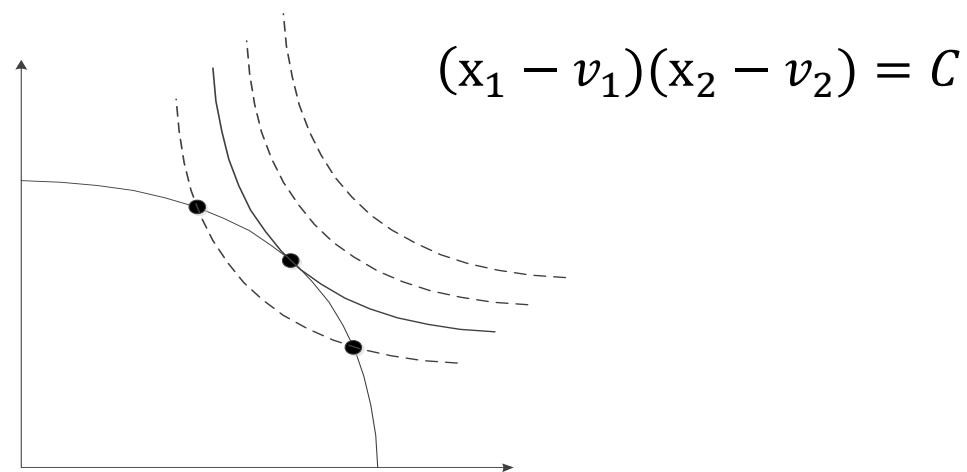
纳什讨价还价(Nash Bargaining)

公理4：等价盈利描述的不变性

- 一个讨价还价问题通过仿射变换变为另一个讨价还价问题，那么原讨价还价解通过仿射变换后也成为新讨价还价问题的解

公理5：无关选择的独立性

- 移除讨价还价解之外的点不会影响讨价还价解的求得

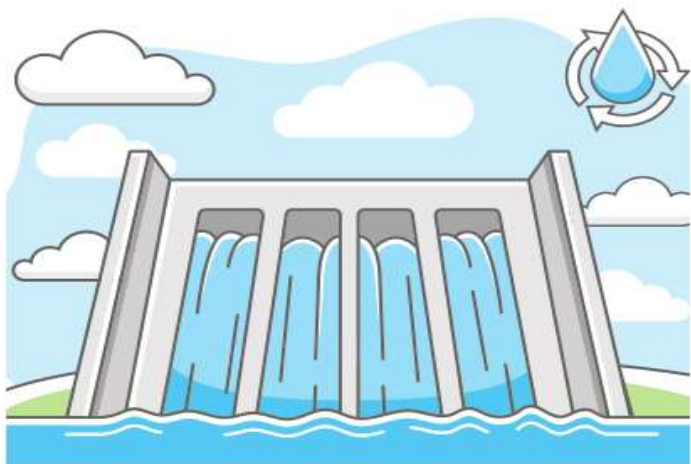


对于两人讨价还价问题 (F, v) ，存在满足公理1-5的唯一讨价还价解



城市输水管道修建问题

- 三个城市（1， 2， 3）计划修建城市用水系统，利用公共的水库资源（Y），城市之间和城市与水库之间的管道铺设成本如下



	城市1	城市2	城市3
水库Y	18	21	27
城市1		15	12
城市2			24

简单计算，从水库到城市1，然后再到城市2和3，成本最小 $18+15+12=45$

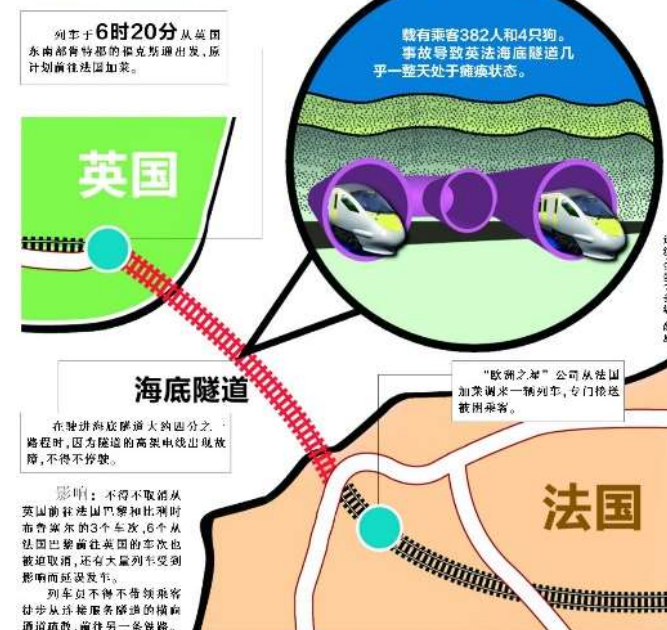
问题：如何在三个城市分摊成本？



英法海底隧道

- 第一次尝试：1802年
- 第一次失败（军事问题）：由于1803年5月16日，英法两国战火不断
- 第二次尝试：1834年
- 第二次失败（政治问题）：拿破仑三世的马车在去往巴黎歌剧院的路上被炸弹袭击
- 第三次尝试：1872年
- 第三次失败（地理问题）
- 第四次尝试：1955年
- 第四次失败（成本问题）

7日上午7时30分



Keep Trying !



英法海底隧道

- 第N次尝试：1981年，英国首相撒切尔和法国总统密特朗在伦敦举行首脑会晤，决定将英法海底隧道的建设和经营承包给私人部门
- 银行团与英法两国的建筑公司联合在两国分别成立了Channel Tunnel Group Limited (CTG) 和 France Manche S.A (FM) 公司，这两家公司再以合伙形式组成欧洲隧道公司 CTG-FM
- 隧道终于在**1994年5月6日**举办了隆重的通车典礼



Success !



程序员鼓励师

某互联网公司今天加班，需要编写一个500行的程序代码，产品经理找了三个程序员来完成，按照完成量发奖金

- 1号屌丝程序员独立能写100行
- 2号大神程序员独立能写125行
- 3号美女程序员能写50行
- 1、2号合作能写270行
- 2、3号合作能写350行
- 1、3号合作能写375行
- 三名程序员共同合作能完成500行



若共有1000元项目奖金，该如何给这三名程序员分配呢？



程序员鼓励师

可能性	加入顺序	第一位的边际贡献	第二位的边际贡献	第三位的边际贡献
1/6	1-2-3	$V(\{1\})=100$	$V(\{1,2\})-V(\{1\})$ $=270-100=170$	$V(\{1,2,3\})-V(\{1,2\})$ $=500-270=230$
1/6	1-3-2	$V(\{1\})=100$	$V(\{1,2,3\})-V(\{1,3\})$ $=500-375=125$	$V(\{1,3\})-V(\{1\})$ $=375-100=275$
1/6	2-1-3	$V(\{1,2\})-V(\{2\})$ $=270-125=145$	$V(\{2\})=125$	$V(\{1,2,3\})-V(\{1,2\})$ $=500-270=230$
1/6	2-3-1	$V(\{1,2,3\})-V(\{2,3\})$ $=500-350=150$	$V(\{2\})=125$	$V(\{2,3\})-V(\{2\})$ $=350-125=225$
1/6	3-1-2	$V(\{1,3\})-V(\{3\})$ $=375-50=325$	$V(\{1,2,3\})-V(\{1,3\})$ $=500-375=125$	$V(\{3\})=50$
1/6	3-2-1	$V(\{1,2,3\})-V(\{2,3\})$ $=500-350=150$	$V(\{2,3\})-V(\{3\})$ $=350-50=300$	$V(\{3\})=50$



程序员鼓励师

- 1号屌丝程序员的Shapley值为：
 - $1/6 \times (100 + 100 + 145 + 150 + 325 + 150) = 970/6$
 - 2号大神程序员的Shapley值为：
 - $1/6 \times (170 + 125 + 125 + 125 + 125 + 300) = 970/6$
 - 3号美女程序员的Shapley值为：
 - $1/6 \times (230 + 275 + 230 + 225 + 50 + 50) = 1060/6$
-
- 根据Shapley值，1号屌丝程序员应该获得的奖金为：
 $1000 \times 32.33\% = \mathbf{323.3}$ 元
 - 2号大神程序员应该获得的奖金同样为**323.3**元
 - 3号美女程序员应该获得的奖金为总奖金的35.33%，即**353.3**元 **最多！**



如何与我们的敌人进行周旋

战略准备 → 战略相持 → 战略反攻



如己
何的开
辟领
属地
于自？



如的
何策
实略
施集
我？
们



如人
何进
和我
我们
周的
旋的
的？
敌



如的
何充
资源
利？
用
我



在截
什，病
么能
地毒
方够
极蔓
进大
行延
地？
拦延

- 我们与对手之间是一个零和博弈，如何找到零和博弈的鞍点，从而能够知道理智对手最可能的行动策略
- 在网络之上，是否存在着第三方可供拉拢的中立组织，利用合作博弈的思想将他们拉拢过来，形成联盟，为最终的战斗胜利积聚力量



第5节 最优化理论

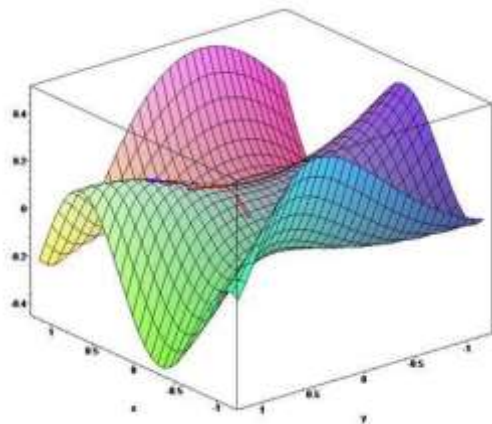
- ✓ 最优性条件
- ✓ 线性规划
- ✓ 凸优化
- ✓ 非凸优化



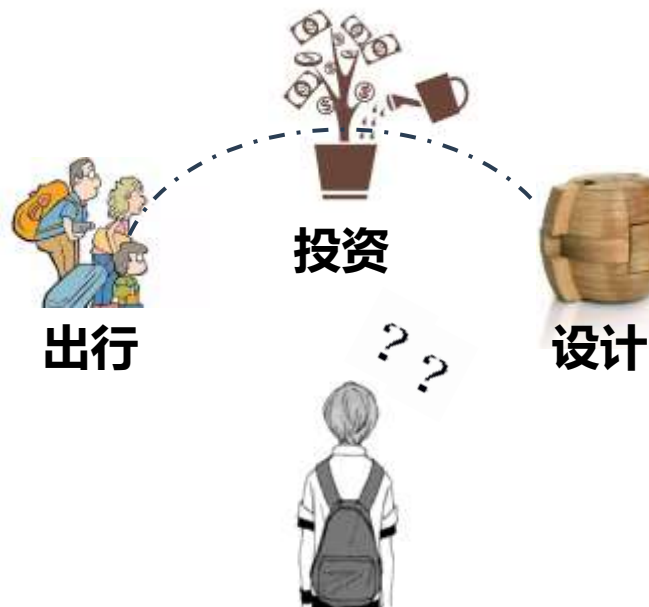
最优化理论



一个数学方法

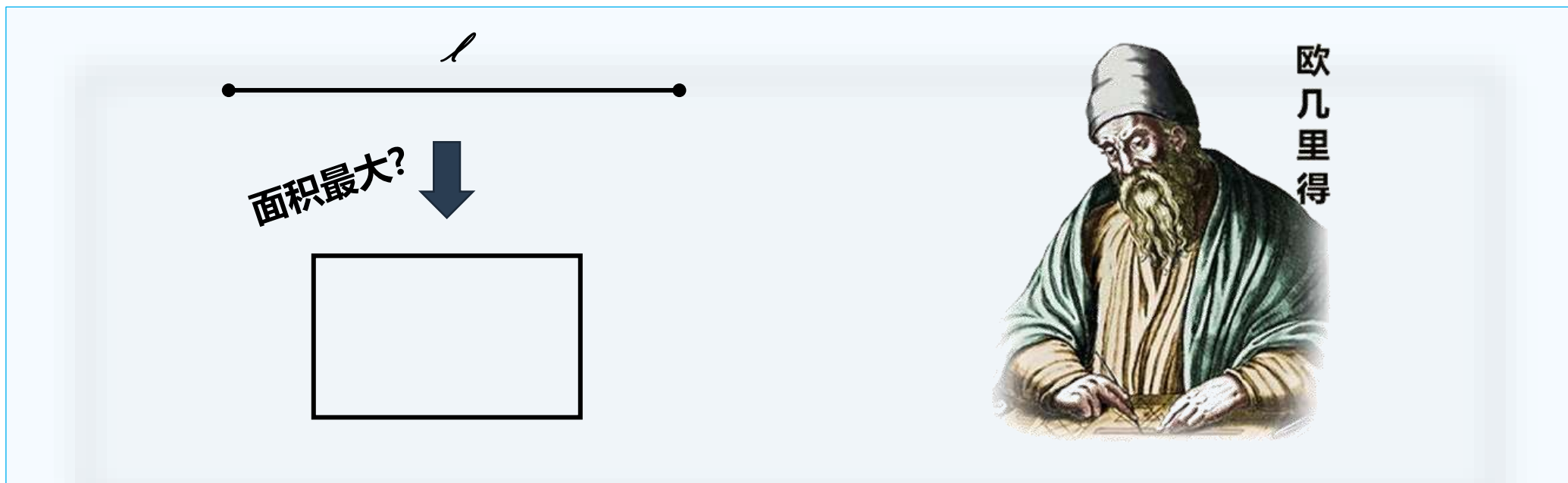


一种生活理念





最优化的起源



记载**最早**的优化问题：欧几里得（Euclid, 公元前300年左右）



最优化的起源

欧几里得问题的抽象

$$\begin{array}{ll}\text{maximize} & x_1 * x_2 \\ \text{subject to} & 2x_1 + 2x_2 = l\end{array}$$



$$\text{maximize } x_1 * \left(\frac{l}{2} - x_1\right)$$

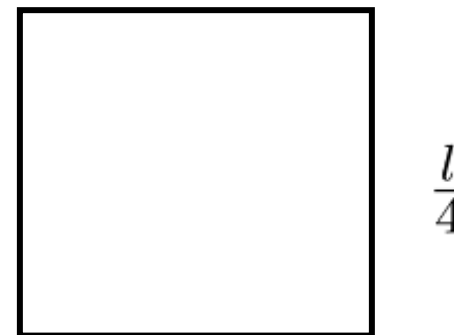


$$x_1 = x_2 = \frac{l}{4}$$



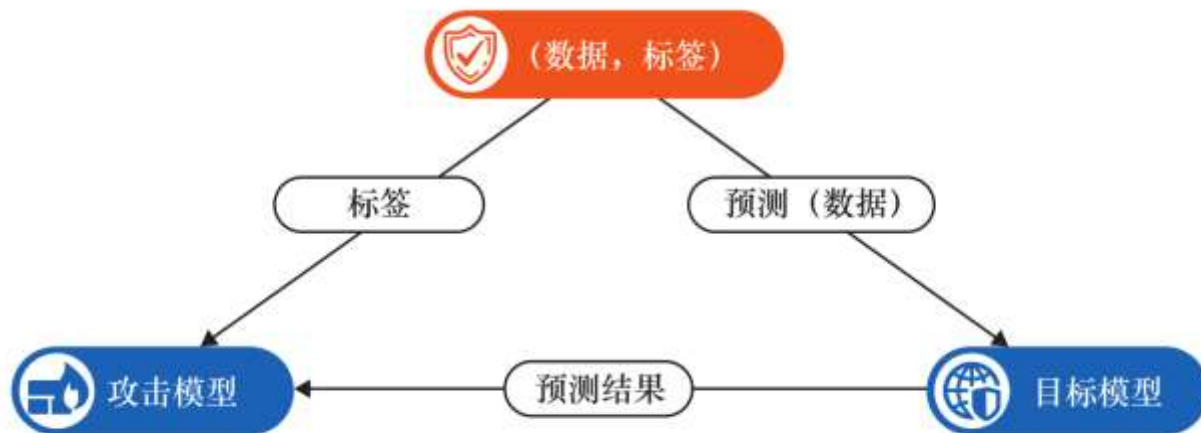
欧几里得

**Here comes the answer:
The square**

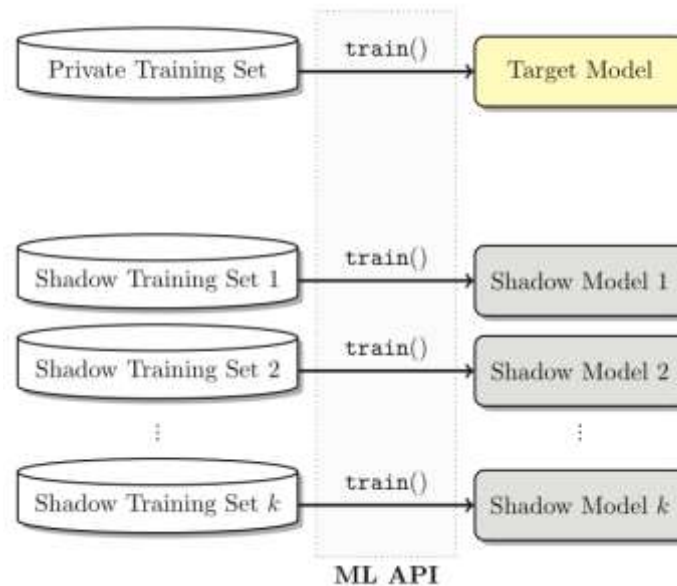




网络安全中的最优化



判断：数据 \in 训练集合？

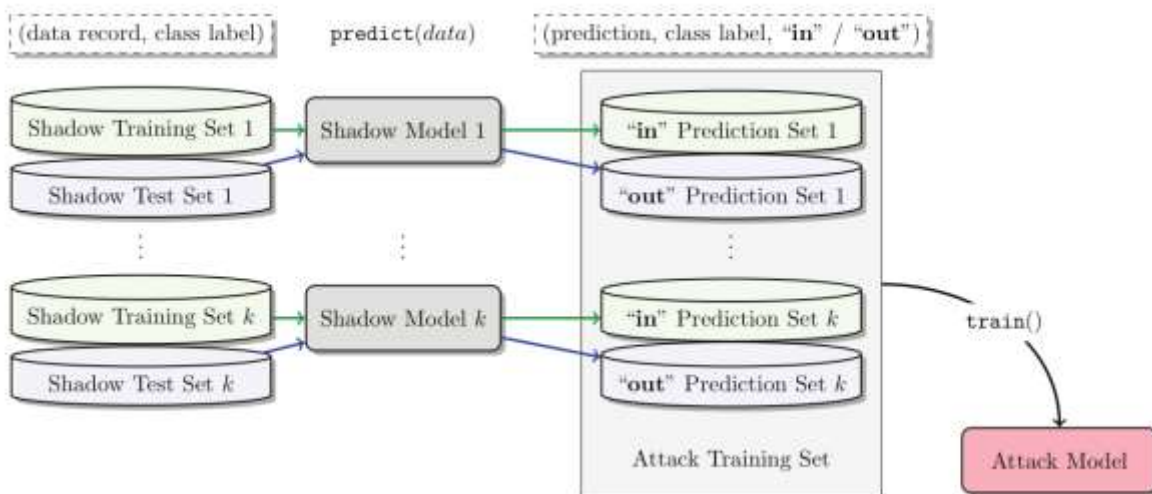


- 对互联网公司提供的黑盒机器学习模型服务进行攻击
- 挑战数据匿名问题，可以使得攻击者预测出相关数据是否在模型训练的数据集中
- 主要思想为优化，找到使得模型**预测信心最大的数据**（爬山算法）



网络安全中的最优化

- 通过爬山算法获得的模拟数据训练**影子模型**，模拟目标模型的行为
- 利用影子模型构建攻击模型数据，并打上标签 **“in”** 或者 **“out”**



Algorithm 1 Data synthesis using the target model

```

1: procedure SYNTHESIZE(class : c)
2:    $\mathbf{x} \leftarrow \text{RANDRECORD}()$   $\triangleright$  initialize a record randomly
3:    $y_c^* \leftarrow 0$ 
4:    $j \leftarrow 0$ 
5:    $k \leftarrow k_{\max}$ 
6:   for iteration = 1  $\dots$  itermax do
7:      $\mathbf{y} \leftarrow f_{\text{target}}(\mathbf{x})$   $\triangleright$  query the target model
8:     if  $y_c > y_c^*$  then  $\triangleright$  accept the record
9:       if  $y_c > \text{conf}_{\min}$  and  $c = \arg \max(\mathbf{y})$  then
10:         if rand() <  $y_c$  then  $\triangleright$  sample
11:           return  $\mathbf{x}$   $\triangleright$  synthetic data
12:         end if
13:       end if
14:        $\mathbf{x}^* \leftarrow \mathbf{x}$ 
15:        $y_c^* \leftarrow y_c$ 
16:        $j \leftarrow 0$ 
17:     else
18:        $j \leftarrow j + 1$ 
19:       if  $j > \text{rej}_{\max}$  then  $\triangleright$  many consecutive rejects
20:          $k \leftarrow \max(k_{\min}, \lceil k/2 \rceil)$ 
21:          $j \leftarrow 0$ 
22:       end if
23:     end if
24:      $\mathbf{x} \leftarrow \text{RANDRECORD}(\mathbf{x}^*, k)$   $\triangleright$  randomize k features
25:   end for
26:   return  $\perp$   $\triangleright$  failed to synthesize
27: end procedure
  
```

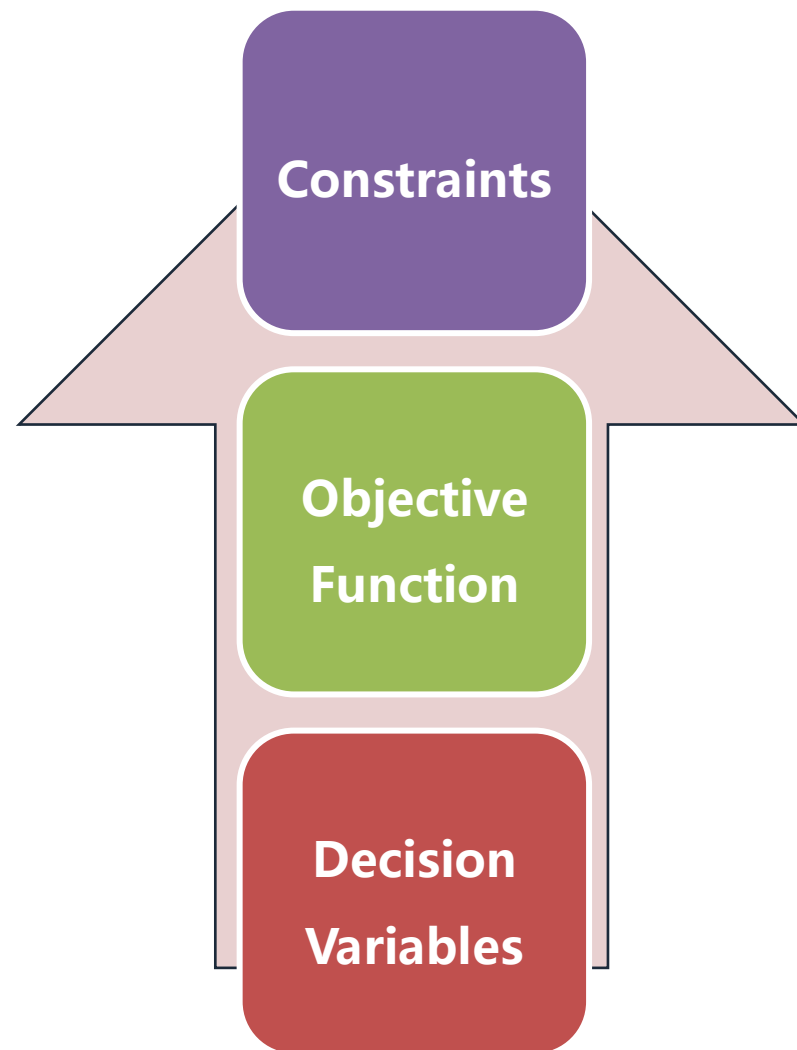


最优化理论的描述

要做的决策是什么?
要达到的目标是什么
决策有什么约束?

minimize/maximize _{x} $f(x)$
subject to $x \in \Omega$

- ▶ x : Decision
- ▶ $f(\cdot)$: Objective
- ▶ Ω : Constraints





最优化理论的描述

优化的思想在人们的生活中无处不在，小到我们生活中的每一个选择，大到国家的战略，都可以分解为这样的三部分。可以说，优化思想是**世间万物的一种基本规律**。

Nothing at all takes place in the universe in which some rule of maximum or minimum does not appear.

-----L. Euler





线性规划

目标函数

$$\max (\min) Z = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n$$

约束条件

$$\left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \leq (= \cdot \geq) b_1 \\ \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \leq (= \cdot \geq) b_m \\ x_1 \geq 0 \cdots \cdots x_n \geq 0 \end{array} \right.$$

约束区域是n维超多面体，目标函数也是仿射函数的规划问题



线性规划

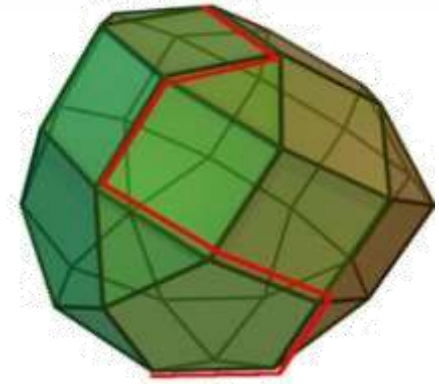


George Bernard Dantzig

November 8, 1914 – May 13, 2005

Dantzig is "generally regarded as one of the three founders of linear programming, along with John von Neumann and Leonid Kantorovich "

- 若线性规划问题有解，则必可在的某个顶点上取得最大值
- 单纯形表的引入，寻找最优顶点





最优性条件

$$\begin{array}{ll}\min & f(\mathbf{x}) \\ \text{s.t.} & g_j(\mathbf{x}) = 0, \quad j = 1, \dots, m, \\ & h_k(\mathbf{x}) \leq 0, \quad k = 1, \dots, p.\end{array}$$

根据优化问题，我们可以引入拉格朗日乘子，将问题**转化为相应的无约束问题**：

$$L(\mathbf{x}, \{\lambda_j\}, \{\mu_k\}) = f(\mathbf{x}) + \sum_{j=1}^m \lambda_j g_j(\mathbf{x}) + \sum_{k=1}^p \mu_k h_k(\mathbf{x})$$

$$\begin{aligned}\nabla_{\mathbf{x}} L &= \mathbf{0} \\ g_j(\mathbf{x}) &= 0, \quad j = 1, \dots, m, \\ h_k(\mathbf{x}) &\leq 0, \\ \mu_k &\geq 0, \\ \mu_k h_k(\mathbf{x}) &= 0, \quad k = 1, \dots, p.\end{aligned}$$

一阶必要条件

Karush-Kuhn-Tucker (KKT)

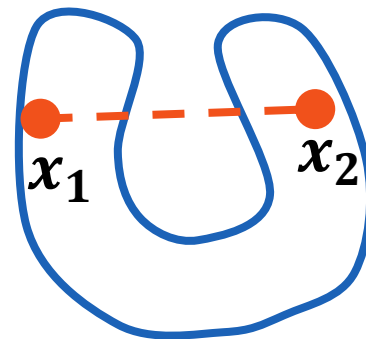
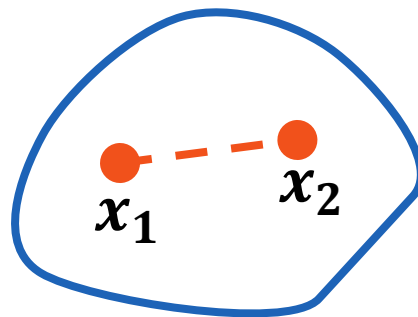


凸优化

- 定义：设 S 是 n 维欧式空间的点集，若 $\forall x_1, x_2 \in S, t \in [0, 1]$ ，都有：

$$X = tx_1 + (1 - t)x_2 \in S$$

则称 S 为凸集

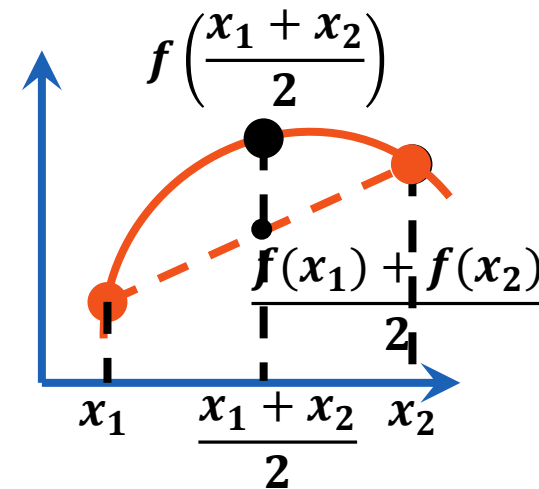
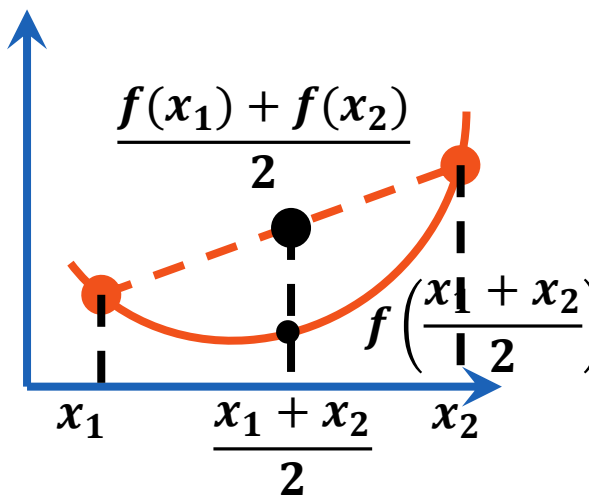


- 定义：设 f 是某个向量空间的凸子集 S 上的实值函数， $\forall x_1, x_2 \in S$ ，

$$X = tx_1 + (1 - t)x_2, \text{ 都有:}$$

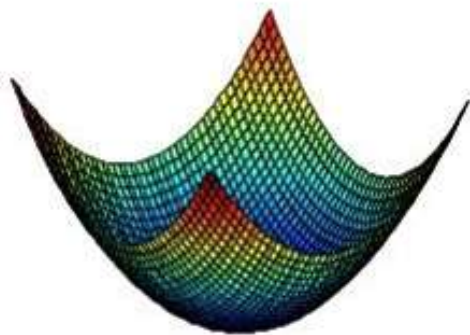
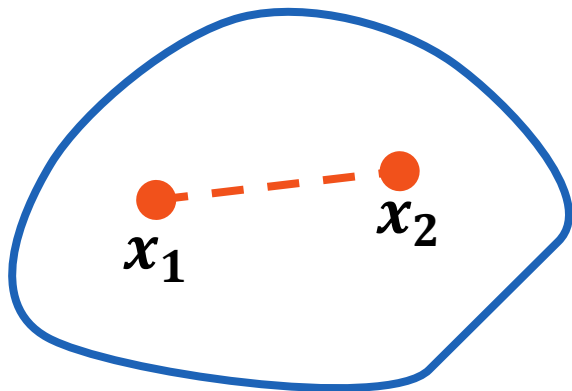
$$f(X) \leq tf(x_1) + (1 - t)f(x_2)$$

则称 f 为凸函数





凸优化

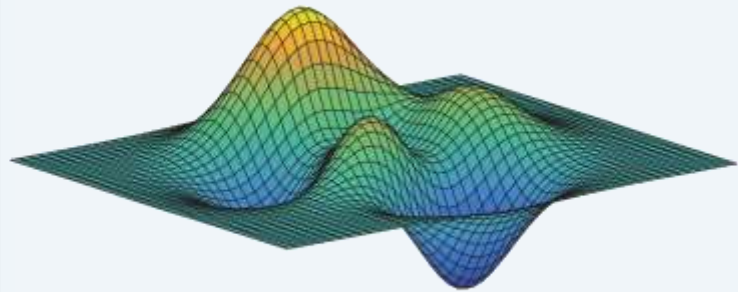


Unique optimum: global = local

- **可行域为凸集且目标函数为凸函数**的优化问题被称为凸优化问题
- 有良好的性质：**局部最优点一定是全局最优点**
- 此时KKT条件变为**充要条件**，KKT点即为全局最优解
- 各种数值优化算法：找到使得目标函数减小的方向，不断移动，直到收敛



非凸优化

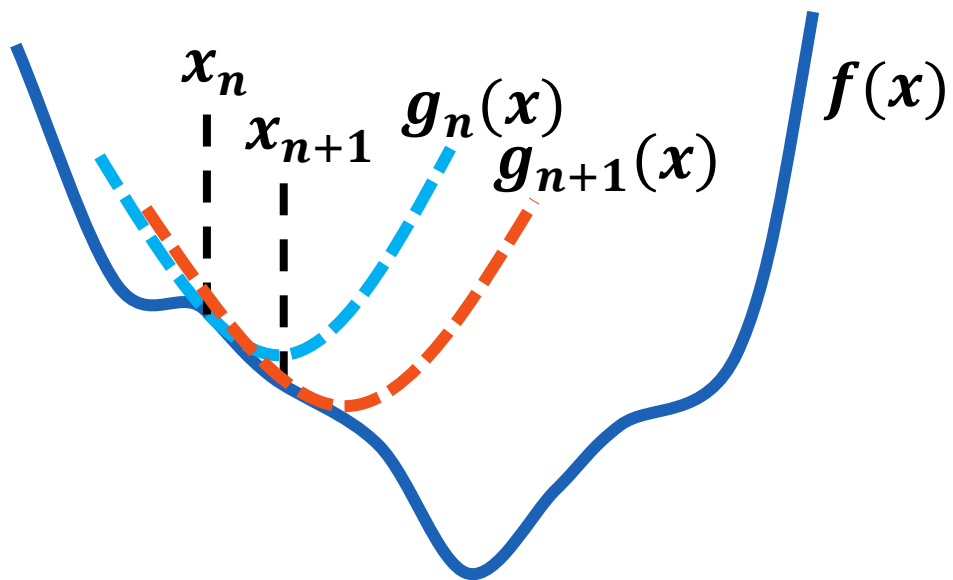


- **Multiple local optima**
- **In high dimensions possibly exponential local optima**

- 非凸优化问题被认为是非常**难求解的**，因为可行域集合可能存在无数个局部最优点，通常求解全局最优的算法复杂度是指数级的 (NP Hard)
- 蒙特卡洛投点法：随机选择任意一个点，通过凸优化算法找到附近的局部最优。如此重复，直到满足一定条件



非凸优化



- 科学的本质是**由易到难**，把简单的问题研究透彻，然后把复杂的问题化为简单的问题
- 梯度下降法求极值： $x_n - hf'(x_n)$

近似泰勒展开，并将二阶项系数置为常数：

$$g(x) = f(x_n) + f'(x_n)(x - x_n) + \frac{1}{2h}(x - x_n)^2$$

求出二次函数的最值，
作为新的迭代点：

$$x_{n+1} = x_n - h\nabla(x_n)$$



基于优化的TCP & AQM

$$\begin{aligned} \max_{x_s \geq 0} \quad & \sum_s U_s(x_s) \\ \text{s.t.} \quad & \sum_{s \in \mathcal{S}(l)} x_s \leq c_l, \forall l \in L \end{aligned}$$

“系统” 优化 问题

- maximize system utility (note: all sources equal)
- **constraint:** bandwidth used less than capacity
- centralized solution to optimization impractical
 - must know all utility functions
 - impractical for large number of sources
 - congestion control as distributed asynchronous algorithms to solve this problem

转化为对偶问题
分布式解决: REM



如何充分利用我们的资源

战略准备 → 战略相持 → 战略反攻



如何开辟属于我们的领地？



如何实施我们的策略？



如何进行我们的周旋？



如何充分利用我们的资源？



在截缓什么，病毒能够蔓延的地方，极大地进行拖延？

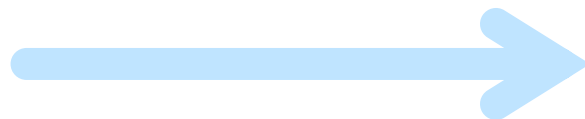
- 无论是人员调配还是物资统筹，都是一个具体的优化问题
- 通过优化问题的抽象、求解，得出内耗最小、外力最大的统筹调配方案，实现最优的作战意图



第6节 概率论与随机过程



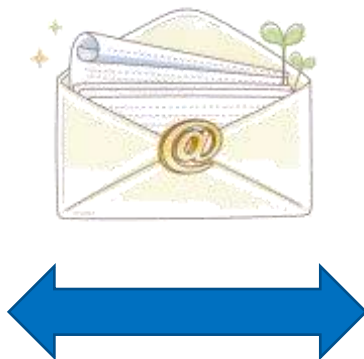
概率与随机的起源



- 1651年，法国一位贵族**梅累**向法国数学家、物理学家**帕斯卡**提出了一个十分有趣的“分赌注”问题
- 这两个赌徒说，他俩下赌金之后，谁先赢满5局，谁就获得全部赌金。赌了半天，A赢了4局，B赢了3局，但时间很晚了，他们都不想继续赌下去了。那么，**这个钱该如何分配？**



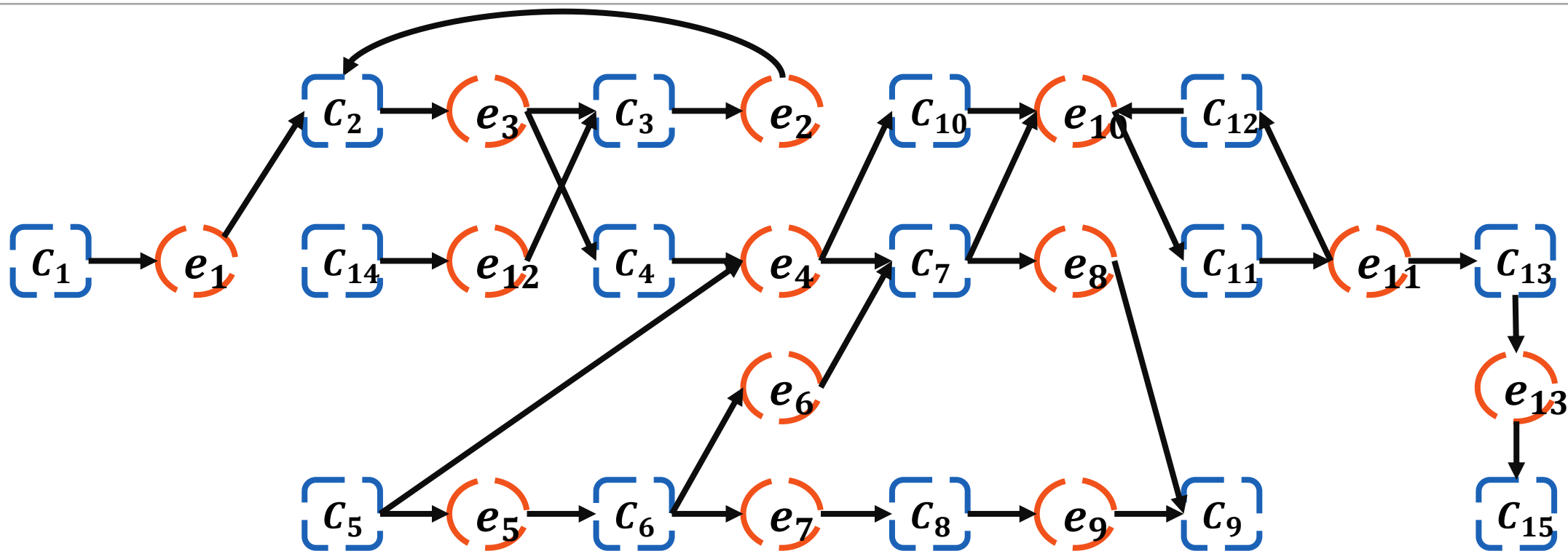
概率与随机的起源



帕斯卡与费马之间的通信，开启了数学家进入概率领域的序幕。他们于1654年共同建立了概率论的第一个基本概念——**数学期望**



网络安全中的概率论



- 通用安全脆弱点评估系统**CVSS(Common Vulnerability Scoring System)**，关注于单个脆弱点的属性量化，提供了在目标网络中攻击者成功渗透的概率
- 对目标网络进行安全评估，需要识别网络中攻击者利用各个脆弱点之间相互关系形成的潜在威胁
- 攻击图结合CVSS系统，形成了所示的**贝叶斯网络**

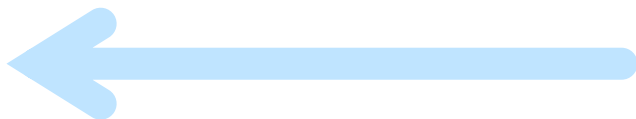


再看交互式零知识证明

Alice (证明者)



You do have the solution!



Bob (验证者)



- After n round, the probability of Alice has a solution will be

$$Pr[\cdot] = 1 - \frac{1}{|E|^n}$$

- If n is very large, Alice will convince Bob

通过 n 次交互，在 n 次 Alice 都提供了正确答案的情况下，事情发生的**概率降到了很小的水平**，于是 Bob 接受了 Alice 掌握正确答案的信息，同时 Alice 关于**正确答案的信息也没有泄露**

如果因为**传输错误**、或者**人为疏忽**，中间有提供了**错误答案**，我们该怎么办？



假设检验

核心思想：

“小概率事件”原理，其统计推断方法是带有概率性质的反证法

- 预先设定小概率值(小到多少是你能接受的“小概率”)
- 作出假设 (一般是二元假设)
- 选择概率计算模型
- 计算如果假设为真的情况下，事件发生的概率
- 如果事件为小概率事件，则推翻原假设，否则接受

Alice (证明者)



Bob (验证者)



- Bob的假设：Alice不知道答案
- 选择概率计算模型：二项分布
- 若假设为真，Alice n 次回答均正确的概率为 $P = \frac{1}{|E|^n}$
- 由于 $\frac{1}{|E|} \leq 1$ ，所以存在某个 n ， n 次之后， P 小于小概率值
- Bob结论：Alice知道答案



交互式零知识证明中的假设检验思想

Alice (证明者)



问题：如果因为传输错误、或者人为疏忽，Alice中间有提供了错误答案，我们该怎么办？

(当交互次数n很大时，这种情况很可能发生)

Bob (验证者)



- Bob的假设：Alice不知道答案
- 选择概率计算模型：二项分布
- 若假设为真，Alice n次回答中有k次错误的概率为：

$$P = C_n^k \frac{1}{|E|^{n-k}} \left(\frac{|E| - 1}{|E|} \right)^k$$

- **若P较大**，达到Bob可接受的水平，则接受假设，Alice不知道答案
- **若P仍然较小**，接近小概率，则继续进行交互，获取更多信息进行观察



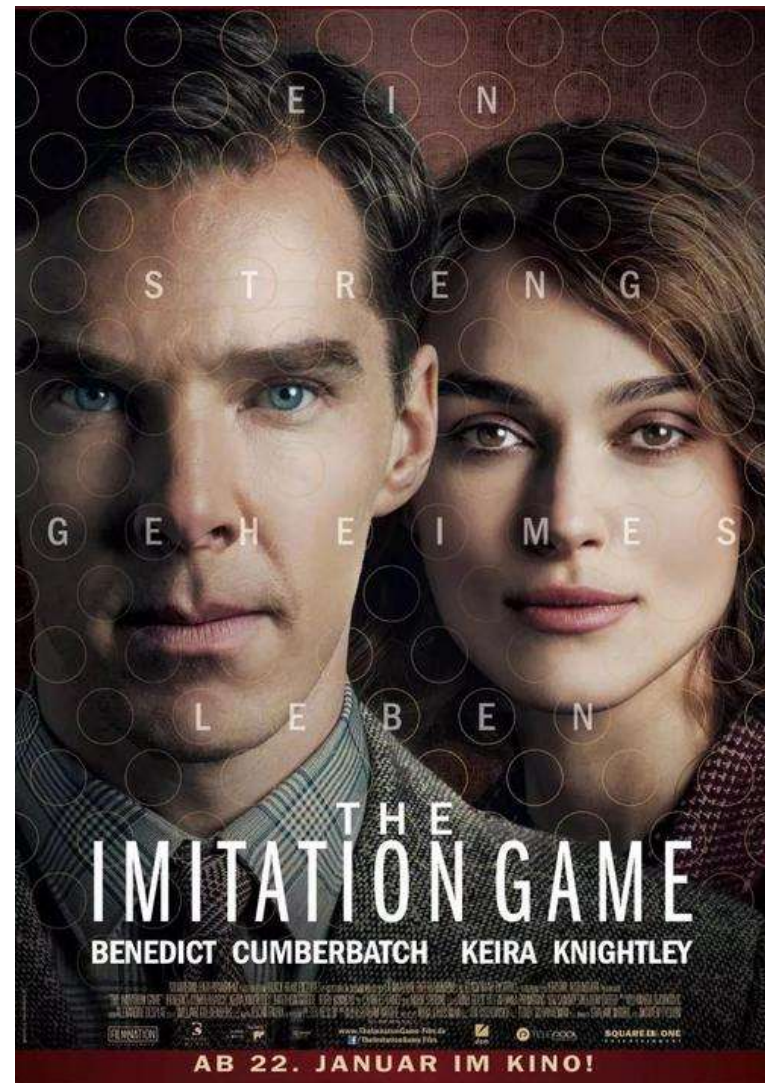
信息加密中的概率问题



- 每个按钮按下时都会带动转子
- 每个转子转动一圈后带动下一个转子转动
- 每个字母一个转子外，再增加几组可调节转子，顺序和初始位置可调

二战中德国配置的Enigma机配备四个转子，不同的组合结果超过了一亿亿种可能性

- 所有密码都存在悖论，既要被自己人理解，又要让敌人无法破解，所以总会存在突破点
- 电影《模仿游戏》中的阿兰·图灵就是利用了初始破译机器的高效运算以及德军在传递过程中的**固定格式**，比如以日期天气开头、以德语Heil Hitler为结尾，从而极大提高了密码的破译概率





网络安全中的撞库攻击



- 黑客通过其他手段**收集互联网已泄露的用户+密码信息**，生成对应的字典表，尝试批量登陆其他网站后，得到一系列可以登录的用户
- 一旦用户为了省事，在多个网站设置了同样的用户名和密码，黑客很容易就会通过字典中已有的信息，登录到这些网站，从而获取一些重要信息

- 密码**相同**的次数越多，被“撞”的概率越**大**；反之，**记忆的难度增大**
- 通过多层映射，降低被破译的概率；同时简化信息记忆难度

- ① 生日
- ② 姓名
- ③ 手机号
- ④ 学号





在什么地方拦截能够最大程度阻止敌人

战略准备 → 战略相持 → 战略反攻



如己
何的
开“
辟领
属地
于”
自？



如的
何策
实略
施集
我？
们



如人
何进
和行
我周
们旋
的？
敌



如们
何的
充资
分源
利？
用我



在截缓
什，病
么能毒
地够的
方极蔓
进大延
行地？
拦延

- 每一个网络节点都有自己的防御系统，根据我们前期与敌人的接触，可以评估每一个节点**被渗透的概率**
- 同时，根据节点周边“敌人”的情况，构建一个贝叶斯网络，来获得所有节点被攻破的概率，从而判断敌人最有可能进攻的位置



第7节 总结和展望



应用理论与基础理论

对于《三体》中关于**基础理论**的说法你怎么看？

应用理论：具体、特性、形象

抽象、泛化



基础理论：抽象、共性、本质

支撑、指导



基础研究成果是整个科学技术的**理论基础**，为应用科学技术提供**理论保证**并指导应用技术向前发展



总结



第一节 新的开始

- 网络安全事件，需要集合不同的理论知识来解决



第二节 图论

- 抽象为着色与匹配问题在网络上开辟根据地



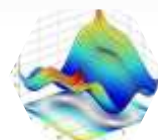
第三节 控制论

- 用随机控制进行初步接触，用反馈调节进行修正



第六节 概率论与随机过程

- 通过节点建模和贝叶斯网络来找出对手的薄弱点



第五节 最优化理论

- 用优化的思想来调度、规划人员和物资



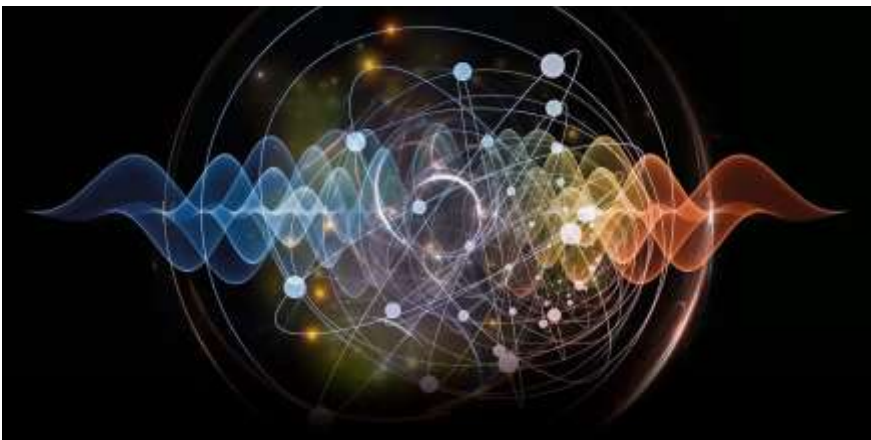
第四节 博弈论

- 用零和博弈的思想来分析双方的策略应对

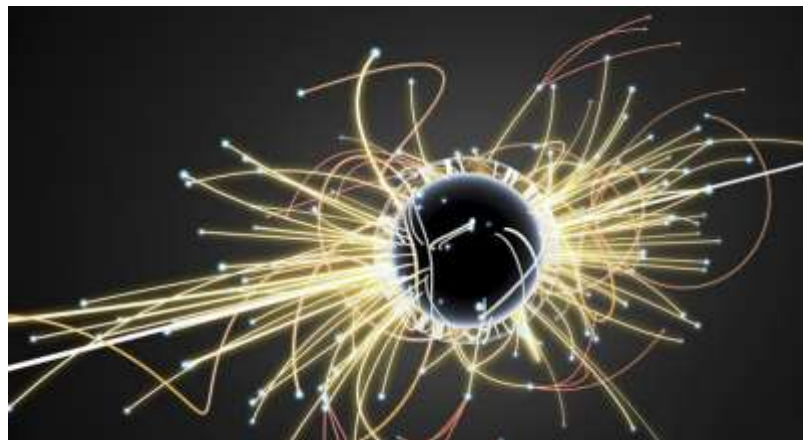


展望

新技术、新应用的出现，网络安全需要新的基础理论支撑



量子通信



量子计算

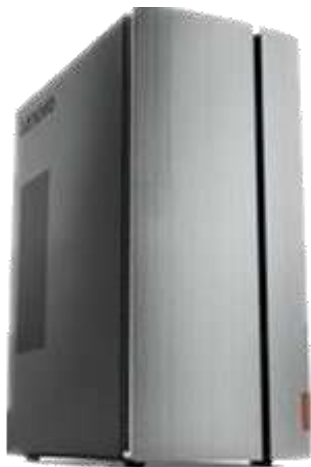


6G应用

- **传统基础理论**如何在新的技术场景、新的网络应用中支撑安全分析
- **新的理论突破**，以应对新的安全场景和安全应用



千里之行，始于足下



- 基础理论是分析网络安全问题的**有力武器**
- 掌握基础理论，可以借**他山之石**攻此山之玉

用**理论工具**武装自己
分析求解网络安全问题