数学建模

浙江大学数学系　谈之奕

tanzy@zju.edu.cn

数学建模概论

数学应用

浙江大学 ZheJiang University

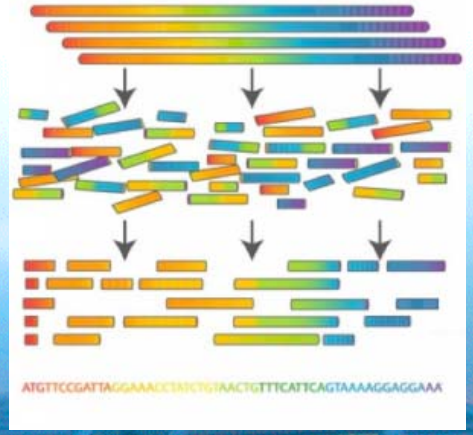
数学建模

- 数学在科学、技术和社会中的作用
  - 数学是自然科学的基础，也是重大技术创新发展的基础。数学实力往往影响着国家实力，几乎所有的重大发现都与数学的发展与进步相关，数学已成为航空航天、国防安全、生物医药、信息、能源、海洋、人工智能、先进制造等领域不可或缺的重要支撑

——摘自科技部办公厅、教育部办公厅、中科院办公厅、自然科学基金委办公室《关于加强数学科学研究工作方案》的通知（国科办基〔2019〕61号）

- 万有引力定律
- 基因测序
- 选举理论

- 计算机
- 大数据



数学应用

浙江大学 ZheJiang University

数学建模


大哉数学之为用

- 宇宙之大、核子之微、火箭之速、日用之繁，无处不用数学

——华罗庚《大哉数学之为用》（原载1959年5月28日《人民日报》第7版）

- “数学用不上”？

任．正如著名数学家 G．B．Dantzig 说的：“对于几乎从来未接触过应用方面的问题，只有纯粹数学背景的人来说，要他懂得如何用数学术语表述一个现实世界的问题，差不多是不可能的．解决现实问题就更难了．”后来中国的实践也证明，纯粹数学家大

——转引自《华罗庚的数学生涯》

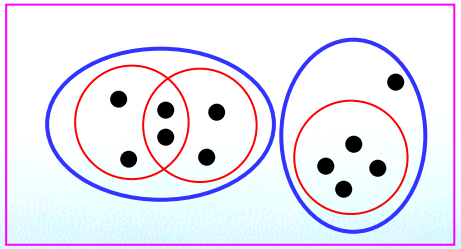
秘密共享

- 秘密共享规定：一保险柜内存有秘密文件，相关5人中有3人及以上在场才能打开
- 保险柜上安装多把锁，每人拥有部分锁的钥匙
- 在保险柜上安装10把锁，每把锁配发3把钥匙，每人手中有6把锁的钥匙
  - 任取3列，必有任何锁的钥匙
  - 任取2列，必缺一把锁的钥匙

	A	B	C	D	E	
1			√	√	√	AB
2		√		√	√	AC
3		√	√		√	AD
4		√	√	√		AE
5	√			√	√	BC
6	√		√		√	BD
7	√		√	√		BE
8	√	√			√	CD
9	√	√		√		CE
10	√	√	√			DE

秘密共享

- “少数”与“多数”
  - 设相关人共有 $2n+1$ 个，任意 n 个组成的“少数”团体不能打开保险柜，任意 $n+1$ 个组成的“多数”团体可以打开保险柜
  - 两个不同的“少数”团体联合可成为多数团体
  - 任一“少数”团体和不属该团体的任一人联合可成为多数团体
- 保险柜上至少需要 $\binom{2n+1}{n}$ 把锁 $\binom{11}{5}=462$
  - 任一“少数”团体至少有一把锁不能打开
  - 任意两个“少数”团体打不开的锁各不相同
- 每个人至少需要 $\binom{2n}{n}$ 把钥匙 $\binom{10}{5}=252$
  - 每个人需拥有他所不属于的所有“少数”团体所打不开的锁的钥匙



Example 1-11 Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet such that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry? To answer

Liu, C.L. *Introduction to Combinatorial Mathematics*. McGraw-Hill, 1968.

秘密共享

浙江大学 ZheJiang University

数学建模

- **Shamir秘密共享机制**
  - 一保险柜的开启密码为整数 X，规定当且仅当相关的 n 个人中有 k 个或以上在场方可开启
  - 随机选择 $k-1$ 个整数 $x_1, x_2, \cdots, x_{k-1}$ 和 n 个互不相同的整数 $c_1, c_2, \cdots, c_n$。计算

$$b_i = f(c_i) = X + c_i x_1 + c_i^2 x_2 + \cdots + c_i^{k-1} x_{k-1}, \ i = 1, \cdots, n$$

  - 将数 c_i 和 b_i 告知第 i 人

Adi Shamir（1952- ）
以色列密码学家
2002年图灵奖得主
2008年以色列奖得主
RSA密码体制发明人之一

Shamir A. How to share a secret. *Communications of the ACM*, 1979, 22(11): 612-613.

秘密共享

- 由若干 c_i 与 b_i 值求 X
  - 若有 k 人在场，线性方程组有唯一解
    - 系数矩阵为 $\begin{pmatrix} 1 & c_1 & c_1^2 & \cdots & c_1^{k-1} \\ 1 & c_2 & c_2^2 & \cdots & c_2^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & c_{k-1} & c_{k-1}^2 & \cdots & c_{k-1}^{k-1} \\ 1 & c_k & c_k^2 & \cdots & c_k^{k-1} \end{pmatrix}$

Vandermonde行列式

$$\prod_{1\le i<j\le n}(c_j - c_i) \neq 0$$

  - 若在场人数小于 k，系数矩阵行数小于列数，线性方程组有无穷多组解，无法得到 X 值

$$b_i = X + c_i x_1 + c_i^{\ 2} x_2 + \cdots + c_i^{\ k-1} x_{k-1},\ i = 1, 2, \cdots n$$

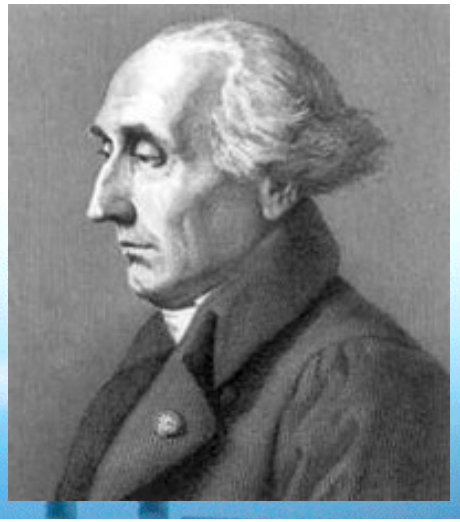
秘密共享

浙江大学 ZheJiang University

数学建模

- 若 $k-1$ 次多项式 $f(c)=X+x_1c+x_2c^2+\cdots+x_{k-1}c^{k-1}$ 经过点 $(c_i, f(c_i)), i=1,2,\cdots,k$，则 $f(c)=\sum_{i=1}^{k} f(c_i)\prod_{\substack{j=1\\ j\neq i}}^{k}\frac{c-c_j}{c_i-c_j}$
  - $X=f(0)=\sum_{i=1}^{k} f(c_i)\prod_{j\neq i}\frac{c_j}{c_j-c_i}$
  - 计算在有限域 $\mathbb{Z}_p$ 内进行

Lagrange插值



Joseph-Louis Lagrange
（1736-1813）
法国数学家、物理学家

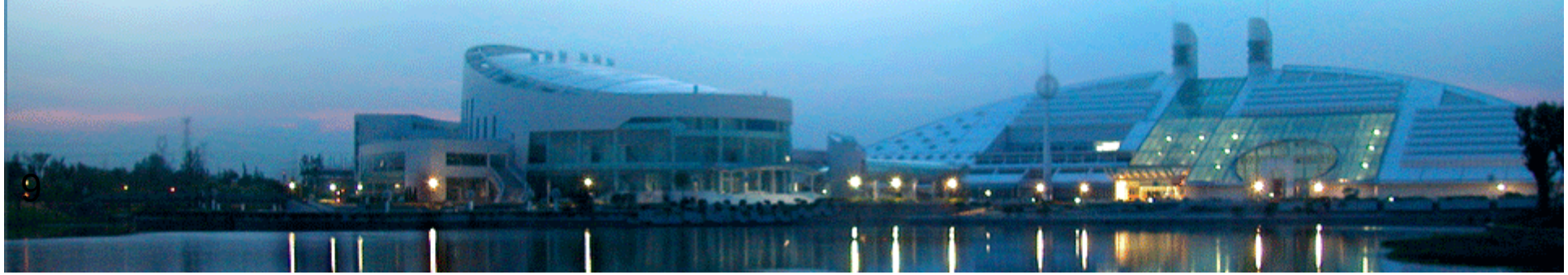
范德蒙其实是一个土生土长的法国人，从他的姓名上看不太出来。1770年11月他正好35岁，在巴黎法国科学院[2]宣读了一篇论文，随后他又在该科学院宣读了三篇文章（1771年他入选该科学院）。这四篇论文就是他的全部数学成果。他的主要兴趣好像是音乐，《科学传记辞典》中记载："据说，当时，音乐家认为范德蒙是一名数学家，而数学家又认为他是一名音乐家。"

范德蒙因以他的名字命名的行列式而广为人知（我将在后面介绍行列式），然而行列式实际上并没有在他的论文中出现，把这功劳归于他似乎是一个误解。总之，范德蒙是一个古怪又有点儿神秘色彩的人物，就

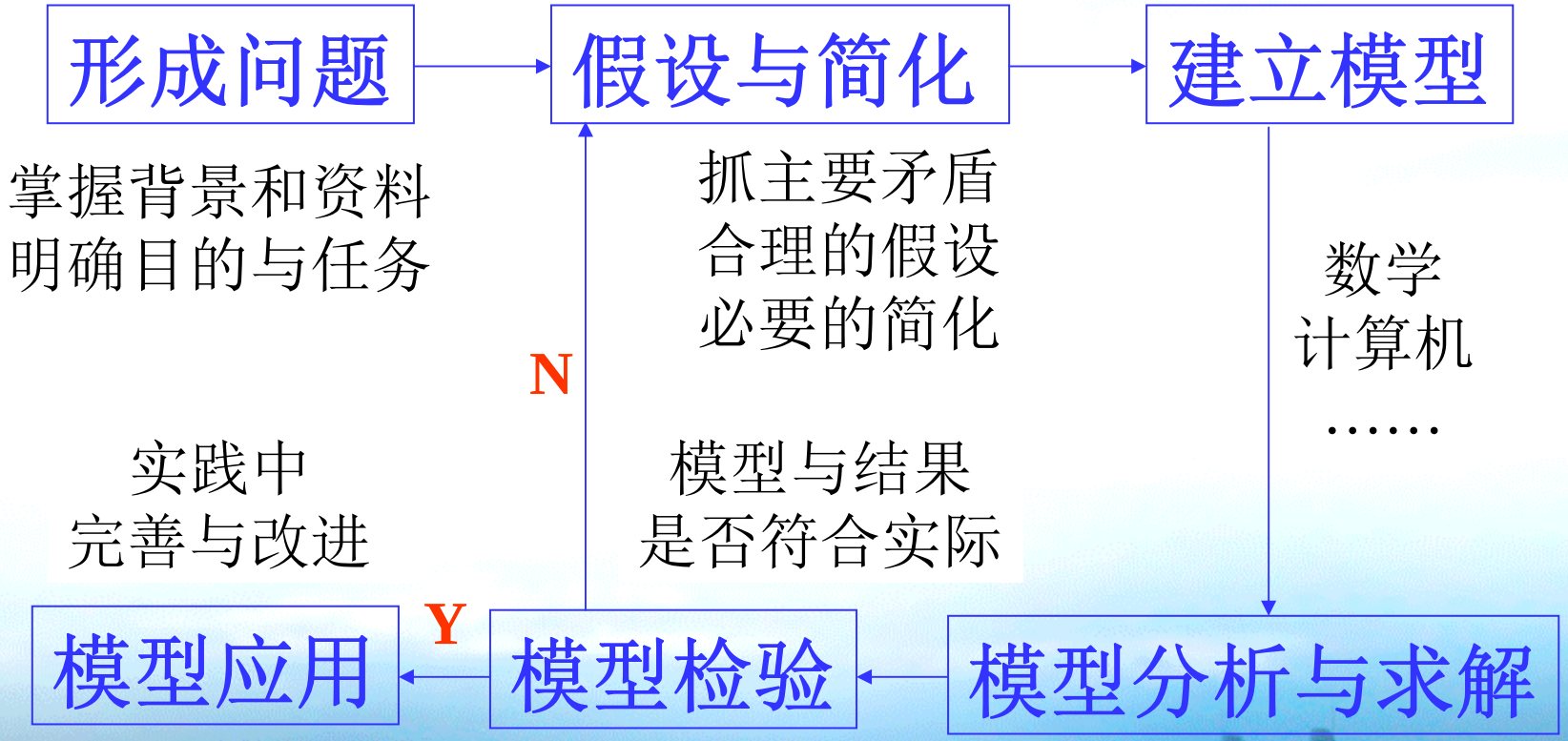
——摘自《代数的历史——人类对未知量的不舍追踪 》

数学模型

- 数学模型是实际问题与数学理论之间的桥梁
  - 模型是对于现实世界的事物、现象、过程和系统的简化描述，或其部分属性的模仿
  - 数学模型（**Mathematical Model**）是针对现实世界的特定对象，为了特定目的，根据特有的内在规律，做出一些必要的简化假设，选用适当的数学工具，得到的一种数学结构
- 建立数学模型的过程，即为数学建模（**Mathematical Modeling**）



数学建模的主要步骤


形成问题
假设与简化
建立模型
掌握背景和资料
明确目的与任务
抓主要矛盾
合理的假设
必要的简化
数学
计算机
……
N
实践中
完善与改进
模型与结果
是否符合实际
Y
模型应用
模型检验
模型分析与求解

数学应用

浙江大学 ZheJiang University

数学建模

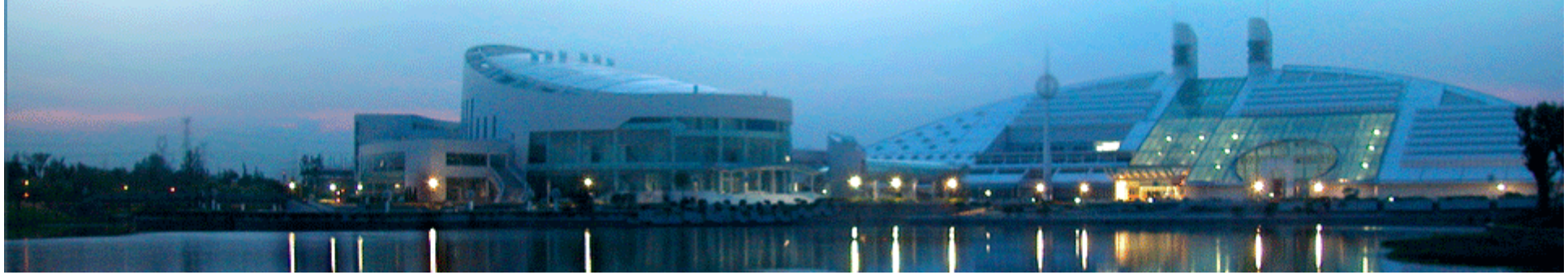
- 数学建模所需的能力
  - 通过交流和查阅文献，归纳、抽象问题的能力
  - 用数学表述、分析与求解问题的能力
  - 使用计算机和数学软件等工具的能力
  - 用语言和文字描述成果，推广应用模型的能力
- 应用数学研究的特点
  - 以实际效果为衡量标准，重视理论指导作用
  - 充分利用已有成果，创造性地为我所用
  - 允许“不严格”，避免不正确
  - 多学科协作，团队攻关

数学基础

浙江大学 ZheJiang University

数学建模

- 数学基础课程（微积分、线性代数、概率论与数理统计、微分方程）
- 微分方程
  - 增长、扩散、竞争
  - 偏微分方程模型
  - 简单控制问题
- 运筹学
  - 连续优化
  - 离散优化、图论
  - 博弈与决策
- 数值计算、反问题
- 随机数学模型
  - 随机过程
  - 排队论、库存论
- 数据分析与处理
  - 数理统计方法
  - 机器学习方法
  - 数据挖掘、可视化
- 综合评价与社会科学中的数学方法
- 计算机应用
  - 启发式算法
  - 模拟与仿真

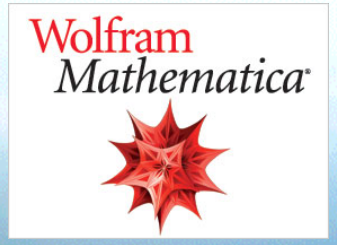


数学软件

浙江大学 ZheJiang University

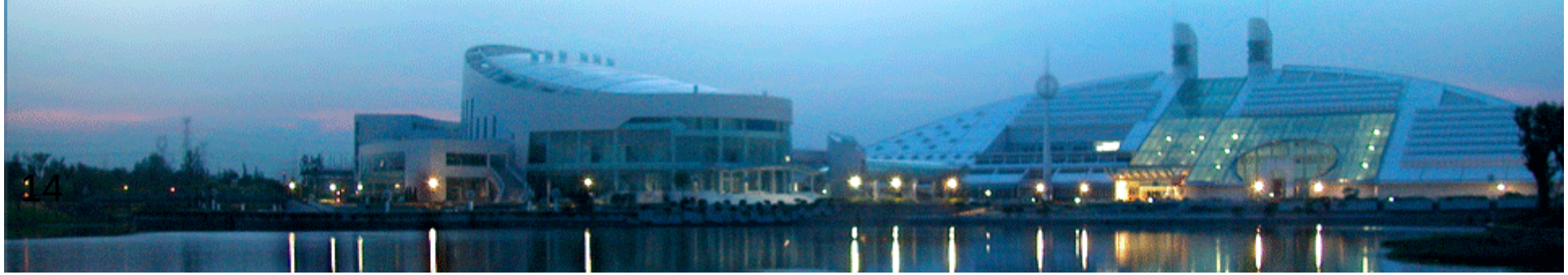
数学建模

- 程序设计语言
- 综合性数学软件
  - **Mathematica**
  - **Matlab**
  - **Maple**
- 专业性数学软件
  - 统计
    - **R**
    - **SPSS**
  - 优化
    - **LINGO**
    - **CPLEX**
    - **Gurobi**



课程概况

- 课程目的与任务
  - 讲授经典数学模型和应用数学方法
  - 介绍数学应用前沿成果，展现数学魅力
  - 培养应用数学知识解决实际问题的能力，加深对数学的理解
  - 通过研究性学习，开展初步科研训练与实践，提升创新能力，提高综合素质
- 学习重点与课程特点
  - 数学知识拾遗补缺，经典模型学习借鉴
  - 科研训练全过程，创新思维初体验
    - 提出问题、发展问题、思考问题、解决问题
  - 数学建模不属单一学科，课程综合性强而连贯性弱；不局限某一学科的数学建模
  - 难立竿见影、不包治百病、忌急功近利、勿依赖他人

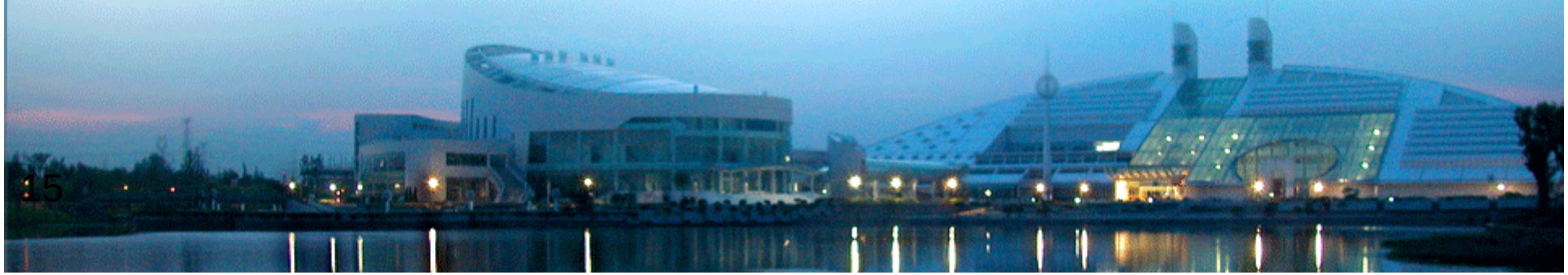


课程概况

浙江大学 ZheJiang University

数学建模

- 课堂讲授内容
  - 数学建模概述
  - 基本数学模型
  - 运筹与统计
  - 数学应用专题
- 课程作业和课外实践
  - 模型讨论、专题研究
  - 研究实践、课程论文
- 课程资料
  - 学在浙大
- 期末笔试：开卷考试
  - “爱课程” 网站 **http://www.icourses.cn/coursestatic/course_6795.html**
- **Email：tanzy@zju.edu.cn**

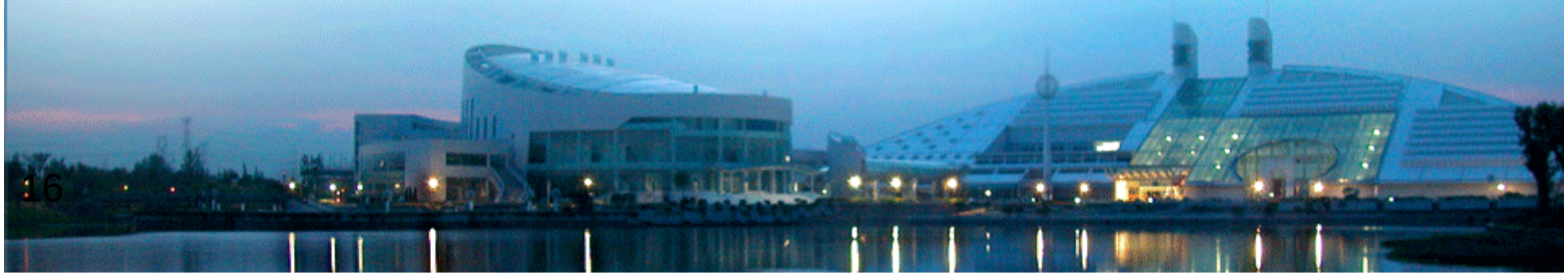


数模学习

浙江大学 ZheJiang University

数学建模

- 数学建模创新中的问题
  - 无法跳出文献窠臼，亦步亦趋
  - 不顾实际情况，缺乏有效评估，生搬硬套已有方法
  - 能学会、能模仿，不能创造、发展
  - 回避问题本质、难点所在，满足于外围、常规、表面
- 参与数学建模学习和实践的建议
  - 不忘初心、积极投入、立足自身、有所作为
  - 脚踏实地、循序渐进、重视基础、结合专业
  - 加强学习、注重实践、增强能力、提升素养




浙江大学
ZheJiang University
谢　谢