

计算机科学与技术系博士学位论文答辩

可满足性问题的算法设计与分析

研 究 生：贺思敏

指导教师：张 钹 教授

1997.5.28

1. 选题背景

- 一个问题：清华大学排课表问题

科学研究要健康发展,应当面向真实问题的求解。

排课表问题 → SAT 问题

- 一个方法：局部搜索

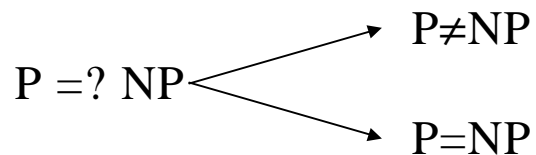
2. 透视计算复杂性理论

SAT: 70 年代 最优解
第一个 NP 完全问题

⇒ 90 年代 近似解
Max-3-SAT: 1.258 可近似
1.038 不可近似($P \neq NP$)

⇒ 启发式算法：有限合理性

- 成果特点：计算机不能做什么
- 技巧特点：不直接构造算法



NP 完全问题在科学研究和实际应用中广泛存在，仅仅指出它们的难解性是不够的，更重要的是正面寻求解决方法，其中的关键是算法的设计与分析。

- 计算复杂性理论的局限性
以不变（算法）应万变（问题），
最坏情况

算法设计应当面向每一个实例的求解，以万变应不变、以万变应万变。

例 1. 《科学美国人》94 年 7 月
“一个 129 位数的密码提前 4 亿亿年被破译”

例 2. 《个人电脑》96 年 9 月
“Netscape 安全防线崩溃”

1995.7.14 RC4 算法 40 位密码加密后的信息

1995.8.15 法国博士生，8 天，盲目猜测，
120 台工作站+2 台超级计算机

1995.9.17 UC Berkeley 两个一年级研究生，
一台工作站，几个小时，破译 129
位密码

例 3. 1997 年 5 月 Deeper Blue 战胜 Kasparov

- 算法设计与分析要走相对独立的道路

“我国的古代数学基本上遵循了一条从生产实践中提炼出数学问题，经过分析综合，形成概念与方法，并上升到理论阶段，精练成极少数一般性原理，进一步应用于多种多样的问题。从问题而不是从公理出发，以解决问题而不是以推理论证为主旨，这与西方之以欧几里德几何为代表的所谓演绎体系旨趣迥异，途径亦殊。”

—— 吴文俊

3. 算法设计：技巧性 → 统一性

- 为什么要追求统一性？

组合问题算法的技巧性

- 局部搜索算法是对付 **NP** 完全问题最有希望的方法

统一性：P 问题，NP 完全问题，连续优化问题

简单性：(S, f, N)，瞎子爬山，一根拐杖

有效性：1990 年，TSP，随机实例， 10^6 城市，
VAX8550，3.8 小时，3.5%

透视计算智能：

模型：优化模型 方法：局部搜索

理论分析：初始点的划分策略的性能
→ 试验设计方法

实验分析：简化、统一、发展局部搜索算法

- 可读性变换是现实而有效的算法设计方法

为什么要变换求解？

他山之石，可以攻玉？

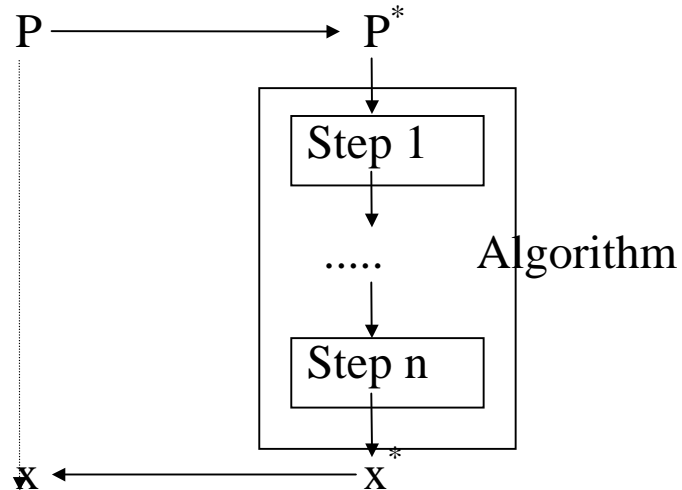
有哪些山头，那些石头？

- 约束满足问题
- 线性及整数规划
- 连续优化(Continuous Optimization)
- 离散局部搜索(Discrete Local Search)
- 多项式方程组求解

.....

如何变换求解？

- 输入变换

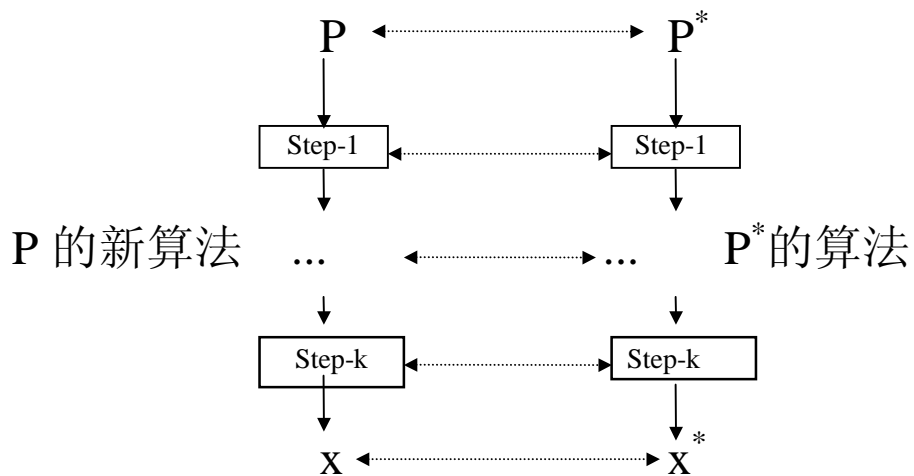


特点：

缺点：

- P^* 难于完全而简洁地表示 P 的特性
- 无法有机结合多种问题求解技术解决同一个问题，因为方法依赖于表示
- 无法揭示不同求解方法的内在联系

- 可读性变换



特点：把方法变过来

只有可读性变换才能真正带来效率

如何实现可读性变换？

方法 1：抽象，使概念和方法脱离具体问题表示形式的束缚，从而可以应用到其他问题上

例 约束满足问题(CSP)到 SAT 问题的可读性变换

强 K 一致性 \longleftrightarrow 有界($K-1$)归结
(Strong k -Consistency) (($k-1$)-Bounded Resolution)

特点：

方法 2：从寻找基本运算的对应入手

例 吴方法求解 SAT 问题的可读性变换

求余操作 \longleftrightarrow 子句归结操作
特征列计算 \longleftrightarrow 子句有限制归结过程

吴方法求解 SAT 问题基本上是以特征列计算为核心的有限制的子句归结过程

- 局部搜索算法与回溯算法的统一

统一多种算法框架

借鉴多种算法技巧

- 再论追求统一性

追求统一性，不仅仅是为了美，更现实地说，这是一种方法。从追求统一性出发，可以找到最相近的问题做类比，从而可以借用其中的概念、方法或从中得到启发，这对于一个科研新手进行有效的思考和寻找合适的出发点尤为重要。

4. 算法分析：理论 → 实验

- 经典的算法分析

渐近复杂性， 最坏情况， 平均情况

局限性： 现实规模下的真实问题
技巧性过强

⇒ 适宜作为一般方法推广吗？

例 模拟退火算法

1983 年 Kirpatrick *et al.*

使用马尔可夫链等复杂工具进行分析的结果是：仅当允许无限多次变换时，模拟退火算法才是一种最优化算法；对最优解任意近似的逼近，对多数组合优化问题都导致比解空间规模还大的变换数，从而导致算法的指数执行时间

1993 年 Ferreira and Zerovnik
渐近， 有限， 并行

1989 年~1991 年 Johnson *et al.*

算法的实验分析将是算法研究的主要手段

- 实验是基础

从基础研究做起的含义是说，一切第一手的资料要有自己的数据积累。别人的实验结果，要经由自己的检验。

—— 何祚庠

…30 年来，重大的发现总数量约 15 件。这是相当惊人的数目。可是除了反质子和中间玻色子外，在这 15 件大发现中，没有一件发现是在事前被理论预测的，这充分表现了物理学实验和理论的发展是分不开的，理论必须通过实验检验，而实验上的发现，对理论常常是起打头的作用。

—— 李政道

“实验计算机科学与工程”

- 实验要讲方法
 - 关于数学的作用
- 实验作为一般方法推广
 - 可操作性，完整性