第十三章
难解问题

姚　刚

中国科学院信息工程研究所

目录

“难解性”理论

什么能披计算或什么不能被计算的讨论，现在要归结到有效计算对无效计算的程度上来进行。

在输入规模的多项式时间里运行的图灵机能计算哪些可判定问题。

下面介绍“难解性”理论，即证明不能在多项式时间里解答的问题的技术。

时间复杂性

如果每当给定图灵机M和长度为n的输入w时，M无论接受与否，都在至多移动$T(n)$步之后停机，则称M具有时间复杂性$T(n)$(或具有“运行时间$T(n)$”)。

$\mathcal{P}$类

如果存在某个多项式$T(n)$和某个具有时间复杂性$T(n)$的确定型图灵机M，使得$L = L(M)$，则说语言L属于$\mathcal{P}$类。

例子：求图的最小生成树的克鲁斯卡尔算法。图的每条边都有整数权。生成树是连通所有顶点而不存在回路的边的子集合。最小生成树在所有生成树中具有最小可能的边权总和。

$\mathcal{NP}$类

如果存在非确定型图灵机M和多项式时间复杂性$T(n)$使得语言$L = L(M)$，且给定M长度为n的输入时，M没有移动序列超过$T(n)$步，则说L属于$\mathcal{NP}$类。

例子：货郎问题。边上带有整数权的图是否具有总权至多为W的“哈密尔顿回路”。哈密尔顿回路是把顶点连接成单个回路且每个顶点恰好出现一次的边的集合。

多项式时间归约

证明在多项式时间里不能解答问题P_2(即P_2不属于$\mathcal{P}$)的主要方法是：把已知不属于$\mathcal{P}$的问题P_1 归约到P_2上。

假设想要证明命题“若P_2属于$\mathcal{P}$，则P_1属于$\mathcal{P}$”。由于断言P_1不属于$\mathcal{P}$，于是可能断言P_2也不属于$\mathcal{P}$。

在从P_1到P_2的变换上施加的限制是：这个变换需要输入长度的多项式时间。

NP完全问题

设L是$\mathcal{NP}$中的一个语言(问题)。如果下列关于L的命题为真，则说L是NP完全的：

1. L属于$\mathcal{NP}$；
2. 对于$\mathcal{NP}$中每个语言L'，都存在着从L'到L的多项式时间归约。

NP完全问题的一个例子是货郎问题。

NP完全问题

由于似乎$\mathcal{P} \neq \mathcal{NP}$，所有NP完全问题都属于$\mathcal{NP} - \mathcal{P}$，所以问题的NP完全性证明就是这个问题不属于$\mathcal{P}$的证明。

定理

若P_1是NP完全的，并且存在从P_1到P_2的多项式时间归约，并且P_2属于$\mathcal{NP}$，则P_2是NP完全的。

定理

若某个NP完全问题P属于$\mathcal{P}$，则$\mathcal{P} = \mathcal{NP}$。

布尔表达式

布尔表达式是用下面这些元素来建立的：

1. 布尔值变元，即这些变元取值1(真)或0(假)。
2. 二元运算符∧和∨，表示两个表达式的逻辑与(AND)和逻辑或(OR)。
3. 一元运算符¬，表示逻辑非。
4. 给运算符和运算对象分组的括号，必要时改变运算的默认优先级：¬最高，其次∧，最后∨。

赋值

给定的布尔表达式E的赋值把真或假指派给E中出现的每个变元。给定赋值T后，E的值记做$E(T)$，这是把每个变元x换成T所指派的值$T(x)$(真或假)，并对E求值的结果。

如果$E(T) = 1$，则赋值T满足布尔表达式E；即赋值T使得表达式E为真。如果至少存在一个满足布尔表达式E的赋值T，则称E是可满足的。

可满足性问题

可满足性问题：给定布尔表达式，这个表达式是可满足的吗？

一般将把可满足性问题称为SAT。作为语言来说，SAT问题是(经过编码的)可满足布尔表达式的集合。

定理 (库克定理)

SAT是NP完全的。

布尔表达式的范式

定义

- 文字就是变元或否定变元。如x和$\neg y$。通常用上划线$\overline{y}$来代替$\neg y$。
- 子句就是一个或多个文字的逻辑或(OR)。
- 如果布尔表达式是子句的逻辑与(AND)，就说这个表达式是合取范式$(或CNF)$。

约束可满足问题

如果表达式是这样一些子句之积，每个子句是恰好k个不同文字之和，则称这个表达式是k合取范式(k-CNF)。

CSAT问题：给定具有CNF形式的布尔表达式，这个表达式是可满足的吗？

kSAT问题：给定具有k-CNF形式的布尔表达式，这个表达式是可满足的吗？

约束可满足问题的NP完全性

定理

CSAT是NP完全的。

定理

kSAT是NP完全的。

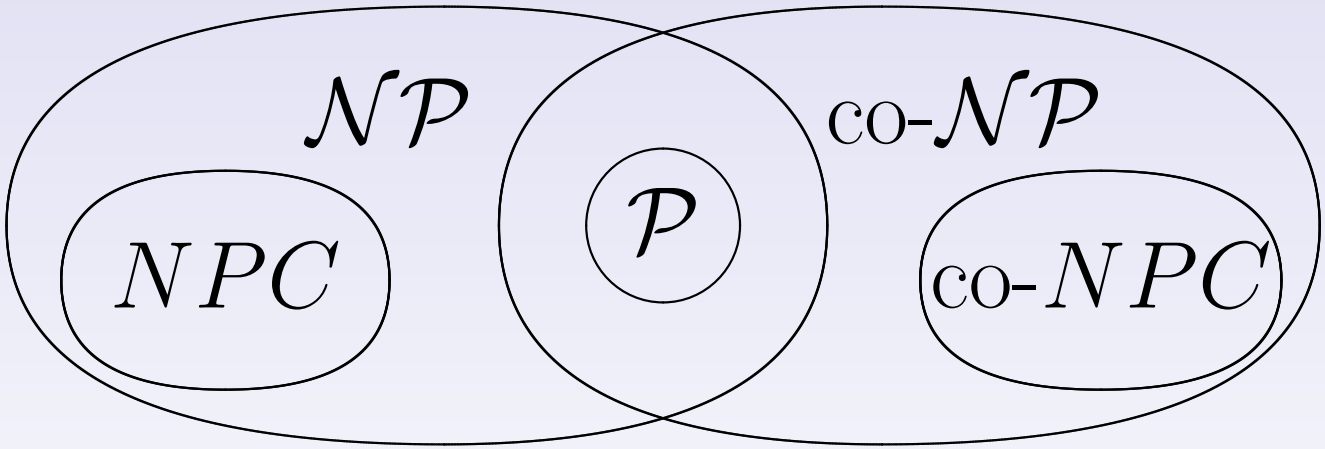
其他的NP完全问题

- 独立集问题
- 顶点覆盖问题
- 有向哈密尔顿问题
- 无向哈密尔顿问题

$\mathcal{NP}$补语言类

$\mathcal{P}$语言类对于补封闭。$\mathcal{NP}$补(co-$\mathcal{NP}$)是那些其补属于$\mathcal{NP}$的语言的集合。

猜测co-$\mathcal{NP}$与其他语言类之间的关系：



定理

$\mathcal{NP}$ =co-$\mathcal{NP}$当且仅当某个NP完全问题的补属于co-$\mathcal{NP}$。

多项式空间图灵机

带多项式空间限制的图灵机是指存在着某个多项式$p(n)$，使得当给定长度为n的输入w时，这台图灵机从不访问超过$p(n)$个带单元。

PS与NPS

定义多项式空间语言类(PS)是由下面这样的语言组成，这些语言都是带多项式空间限制的确定型图灵机M所接受的语言$L(M)$。同样定义非确定型多项式空间类(NPS)由下面这样的语言组成，这些语言是非确定型的带多项式空间限制的图灵机M所接受的语言$L(M)$。

显然$PS \subseteq NPS$，因为每一台确定型图灵机也是非确定型的。

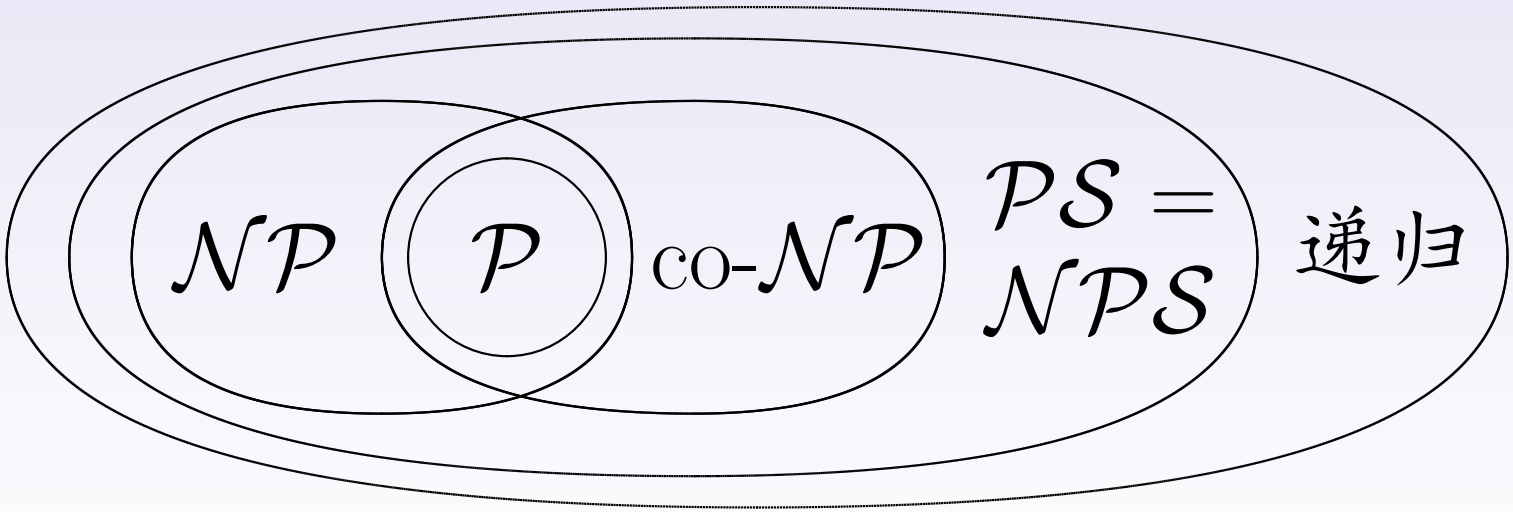
定理

显然$\mathcal{P} \subseteq \mathcal{PS}$，$\mathcal{NP} \subseteq \mathcal{NPS}$。

定理 (萨维奇定理)

$\mathcal{PS} = \mathcal{NPS}$。

多项式空间类的位置：



PS完全性

如果P属于$\mathcal{PS}$，并且所有的$\mathcal{PS}$中的语言L都能在多项式时间内归约到P，则称问题P对$\mathcal{PS}$是完全的(PS完全的)。

注意，虽然考虑多项式空间而非时闻，但PS完全性的要求却类似于NP完全性的要求：归约必须在多项式时间内完成。

定理

定理

假设P是PS完全问题。那么：

- 若P属于$\mathcal{P}$，则$\mathcal{P} = \mathcal{PS}$。
- 若P属于$\mathcal{NP}$，则$\mathcal{NP} = \mathcal{PS}$。

例子：带量词的布尔公式(QBF)问题。

定理

QBF问题是PS完全的。

量词

带量词的布尔公式就是增加了$\forall$(所有)和$\exists$(存在)运算符的布尔表达式。表达式$(\forall x)(E)$的含义是：当把E中所有出现的x都换成1(真)时E为真；并且当把E中所有出现的x都换成0(假)时E也为真。表达式$(\exists x)(E)$的意思是：要么当把E中所有出现的x都换成l(真)时E为真；要么当把E中所有出现的x都换成0(假) 时E为真；要么在两种情况下时E都为真。

QBF问题

形式上，定义带量词的布尔公式如下：

1. 0(假)、1(真)和任何变元都是QBF。
2. 如果E和F是QBF，那么(E)、$\neg(E)$、$(E)\wedge(F)$、$(E)\vee(F)$都是QBF。
3. 如果E是QBF，且不含有变元x的量化，那么$(\forall x)(E)$和$(\exists x)(E)$都是QBF。

QBF问题：给定一个无自由变元的QBF，其值是否为1？

随机化图灵机

随机化图灵机是多带图灵机的变体：第一条带记录输入；第二条带开头的单元中也是非空格，整条带上都覆盖着0和1，每一个都是独立地和随机地选择的，1/2概率为0，1/2概率为1，第二条带将被称为随机带。第三条带和后面的带(假如用到的话)开始都是空白带，并且被图灵机在需要时用作“草稿带”。

随机多项式类($\mathcal{RP}$类)

如果语言L属于$\mathcal{RP}$类，语言L必须被随机化图灵机M在下列意义下接受：

1. 如果w不属于L，那么M接受w的概率是0。
2. 如果w属于L，那么M接受w的概率至少是$1/2$。
3. 存在多项式$T(n)$，使得如果输入w长度为n，那么无论随机带的内容是什么，M的所有运行都在至多$T(n)$步后停机。

零错误概率多项式类(ZPP类)

ZPP类是基于一种总是停机，并且停机的期望时间是输入长度的某个多项式的随机化图灵机。

如果这种图灵机进入接受状态(因此在这个时刻停机)，就接受输入，而如果停机不接受，就拒绝输入。

ZPP类的定义几乎与P的定义相同，不同之处在于，ZPP允许图灵机的行为与随机性有关，并且度量的是期望运行时间而不是最坏情形运行时间。

$\mathcal{RP}$与$\mathcal{ZPP}$

如果L属于$\mathcal{ZPP}$，那么$\overline{L}$也属于$\mathcal{ZPP}$。

但是$\mathcal{RP}$对补封闭却并不是显而易见的，因为定义非对称地处理接受和拒绝。因此，定义$\mathcal{RP}$补(co-$\mathcal{RP}$)类为使得$\overline{L}$属于$\mathcal{RP}$的那些语言L的集合。

定理

$\mathcal{ZPP} = \mathcal{RP} \cap$ co-$\mathcal{RP}$。

与$\mathcal{P}$和$\mathcal{NP}$的关系

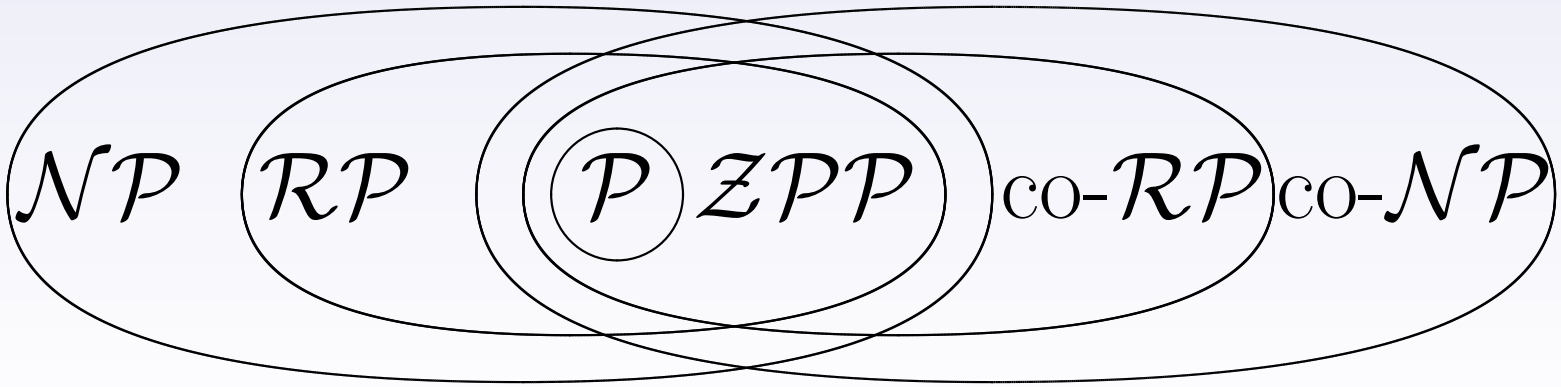
定理

$\mathcal{P} \subseteq \mathcal{ZPP}$。

定理

$\mathcal{RP} \subseteq \mathcal{NP}$。

$\mathcal{ZPP}$和$\mathcal{RP}$与其他语言类的关系：



谢谢！

主 讲 人： 姚 刚

电子邮箱： yaogang@iie.ac.cn