

文章编号:1674-2869(2015)10-0073-06

NP 完全问题研究及前景剖析

杜立智,陈和平,符海东

武汉科技大学计算机科学与技术学院,湖北 武汉 430065

摘要: P vs. NP 是理论计算机领域最重要的课题之一,而其中的核心是 NP 完全问题. 由于该问题所涉及的概念复杂抽象,对它们的理解存在不少谬误,许多已发表的研究论文都包含着这些谬误. 主要是:NP、NP 完全概念理解谬误,确定性及非确定性图灵机的概念模糊不清,P 与 NP 关系的误读,NP 问题研究方向的误导等. 本文分析了这些谬误,并揭示了相关概念的实质. 通过不同角度多方位分析,对 NP 完全问题可能的解决途径和研究方向,提供了启发式思路.

关键词: 确定性图灵机;非确定性图灵机;NP 完全问题

中图分类号: TP3-0

文献标识码: A

doi: 10. 3969/j. issn. 1674-2869. 2015. 10. 014

0 引言

对 P 和 NP 问题的研究,关键有两个方面,第一是对相关概念的正确理解和把握,第二是正确的研究方向与正确的研究方法. 对于第一点,由于相关概念相当复杂抽象,存在着许多理解上的谬误. 甚至一些翻译过来的教科书都存在这些谬误,从而影响了该专业的学生正确理解掌握相关概念. 对于第二点,关键是倾向于以 NP 等于 P 为出发点还是相反. 不同的出发点,对研究的成功与否,起着至关重要的作用.

而在所有 NP 相关问题中,NP 完全无疑是最重要的概念. 事实上,对 NP 完全及其相关概念的透彻理解,是深入研究 NP 问题,尤其是研究 NP 与 P 的关系问题的关键. 谈到 NP 完全,又不能不涉及到多项式归约.

本文的目的是,通过分析 NP 问题的核心概念,并通过抽象定义的解析结合对认识谬误的剖析,揭示其实质. 本文的关键点是,深入剖析 NP 完全问题时间复杂度的逻辑内涵,同时通过对多个实际问题的分析,给出解决 NP 完全问题的启发式思路,从而为该领域的研究者在概念和研究方向的正确把握上提供参考.

1 NP 和 NP 完全问题的起源与基本思想及其影响和发展

NP 问题是随着计算复杂性理论的产生而出现的. 根据计算复杂性理论,所有科学问题按其解决时间可分为三大类:多项式类、指数类和不可解类. 但要确定某个具体的问题到底属于哪一类,往往并非一件容易的事情,尤其是对少数难度大的问题^[1-2].

在理论计算机领域,对这三类问题的研究本来就浩瀚和深不可测,随着 NP 问题的出现,事情就更复杂了. NP 问题是与确定性图灵机和非确定性图灵机的概念一起出现的^[3]. 这两个概念相当抽象,极难透彻理解掌握,从而更加为 NP 问题蒙上了一层神秘色彩.

通俗地讲,NP 问题是“多项式验证”问题. 也就是说,若是有了某个 NP 问题的解,要判断这个解是否正确,这个判断可以在多项式时间内完成. 至于求解这个问题到底需要多少时间,先撇开.

自从 NP 问题出现以后,学术界长时间对此进行了大量的投入及研究,尽管取得了不少研究成果,由于 NP 问题的难度和深度,迄今为止,依然不

收稿日期:2015-08-17

基金项目:湖北省自然科学基金项目(2014CFC1121)

作者简介:杜立智(1964),男,湖北黄冈人,副教授,硕士. 研究方向:计算机算法;计算数学;计算复杂性.

能确定 NP 到底属于上述三类问题中的哪一类. 可以确定两点, 其一是 NP 问题空间复杂度是多项式, 其二是, NP 问题时间复杂度的上限是指数型. 所以, 任何 NP 问题要么是多项式, 要么是指数型^[4], 而不可能是不可解的问题. 不过, 要确定 NP 到底是不是属于多项式, 确定这一点本身倒可能是不可解问题. 不少专家提出了这样的判断和疑问.

1937 年, 英国计算机科学家, 同时也是计算复杂性理论开山鼻祖的图灵提出了一种自动机模型, 后来被人们称作图灵机, 并论证了图灵机的可计算功能. 图灵机模型的提出不仅为现代计算机的设计奠定了理论基础, 同时也成为引出和研究 NP 问题的工具.

后进一步分为确定性图灵机(DTM)和非确定性图灵机(NDTM)两类. 这两个概念在教科书中的定义高度抽象, 难以把握. 笔者在这里用通俗的语言加以剖析. 确定性图灵机是现代计算机的理论模型, 可以认为现代计算机是对图灵机理论模型的实现. 其计算功能与现代计算机等价, 但还是有根本的不同, 前者更抽象. 笔者曾经用确定性图灵机进行了编程练习, 解决同样的问题, 比当今流行的计算机语言编程要难得多. 而非确定性图灵机则纯属理想的理论模型, 现实中无法实现. P 类问题也定义为在确定性图灵机上能在多项式时间内解决的问题; NP 类问题则是在非确定性图灵机上能在多项式时间内解决的问题.

非确定性图灵机的最大特点就是具有并行运算能力. 但请注意正确理解它的关键是, 这个并行并不是无限制的. 它只能进行“分叉”式的并行, 而不能按许多甚至无数平行线“平行”方式地并行. 若是后者, 那非确定性图灵机就不仅能解决 NP 问题, 指数型问题也能一块解决了. 用一颗 n 层的 k 叉树来描述确定性非确定性图灵机的区别无疑能说明问题, 可以肯定所有 NP 问题都可以翻译成这个模型. 对于这样一棵树, 其节点数目是指数型, k 的 n 次方. 当然这些节点之间有统一的联系规律, 这个规律信息是多项式. 要寻找其中一个点, 以及从顶点到这个点的一条路径, 非确定图灵机从顶点开始向下, 在每一个分叉处能并行地同时向所有分支走下去, 从而, 最多 n 步就能达到目的; 而确定性图灵机无并行能力, 它需要遍历整个树, 才能保证找到目标. 当然, 也不排除有高超的算法使其能快速得到结果.

显而易见, 所有多项式问题, 也就是 P 类问题, 肯定属于 NP. 因为能在多项式时间内计算出结果的, 必然也能在多项式时间内验证结果. 但 NP 是否属于 P 成了该领域的最大难题, 迄今无法确定. 该问题的解决不仅能在该领域带来理论上的重大突破, 并且也能对许多重要的问题的实际计算具有意义.

1971 年, NP 问题的研究取得了里程碑的突破. 加拿大著名计算机科学家史蒂文-库克证明了存在具有 NP 完全性质的 NP 问题^[5], 这就是可满足性问题(SAT), 它也是人类发现的首个 NP 完全问题(NPC). 所谓某问题具备 NP 完全性, 也就是, 任何 NP 问题的求解都可以多项式转化到对该问题的求解. 库克构造了一般 NP 问题, 也就是任意 NP 问题多项式转化为 SAT 问题的转化方法和公式, 从而完成了 NP 完全的证明. 其逻辑结果是: 如果能得到可满足性问题的多项式时间算法, 那就意味着所有 NP 问题都具有多项式时间算法, 即 NP 等于 P. 请注意证明某 NP 问题具有 NP 完全性, 通常是一道艰难的工作, 普通的 NP 问题并不具备这一特性. 而大量的 NP 问题其实就是非常简明的 P 问题. 不少论文书刊中, 经常使用这样的说法: 某问题是 NP, 故无有效算法. 这当然是一种谬误, 是混淆了 NP 与 NP 完全的概念.

NP 和 NP 完全问题的出现, 对计算机算法和计算复杂性领域, 产生了重大而深远的影响.

随着第一个 NP 完全问题的发现和证明, 兴起了对这类问题之间的多项式转化研究. 在教科书中通常将这种转化称为“归约”^[6]. 注意理解多项式归约必须把握两个关键点: 一是转化本身所需的时间是多项式, 二是转化后对原问题计算规模的扩大, 不超出多项式的范围. 例如, 若需要将具有 n 个变量的 3SAT 问题按多项式规约转化为对另一 NP 问题的求解, 那么, 转化所需的时间不能超出 n 的多项式函数, 同时, 设转化后后一问题的大小规模为 m , m 也不能超出 n 的多项式函数. 若是 m 在 n 的基础上呈指数型放大, 即使转化本身所花的时间很快, 那当然也不能称作多项式归约.

长期以来, 多项式转化的研究一直经久不衰. 它主要有两个方面的价值. 从 70 年代初开始, 前期的研究主要是为了发现 NP 完全问题. 那时候每发现一个 NP 完全问题, 就是一个较轰动的大成果. 如今这个已经不那么重要了. 但由于 NP 完全问题

之间的多项式转化性质,若得到了一个问题的高效算法,则可以通过转化得到其他问题的高效算法.因而前一类目的的研究已经显著降温,后一类目的的研究则更有实用价值.

这就是 NP 完全问题的意义和实质.

关于 NP 完全问题,还有一个重要概念就是伪多项式时间算法.举例来讲,整数背包问题:给定一些整数 $C_j, j=1, 2, \dots, n$, 以及整数 b , 是否存在整数 $X_1, \dots, X_n \geq 0$ 使得 $\sum_{j=1}^n C_j X_j = b$? 该问题是经典的 NP 完全问题, 但该问题存在针对参数 n 和 b 的多项式时间算法, 称伪多项式时间算法. 也就是说, 必须限定 b 的大小为 n 的多项式, 该问题才具有多项式时间算法. 而当 b 很大, 为 n 的指数幂时, 按同样方法得到的算法的时间复杂度就不是多项式, 而是指数型了. 一些研究者不理解这一点, 花了大量的时间和精力, 找到了该问题的在限定了 b 的大小的前提下的多项式时间算法, 就真的以为已经解决了 NP 是否等于 P 的问题. 其实是大谬误.

2 关于 NP 完全问题时间复杂度的争论

首先讨论 NP 完全问题时间复杂度的一些特点. 一般来说, 对于所熟悉的许多多项式时间问题, 其时间复杂度的曲线很光滑. 也就是说, 局部范围的输入数据, 往往具有整体时间复杂度的特性. 例如, 对于著名的冒泡排序算法, 其时间复杂度在最坏的情况下是 n 的平方, 在最快的情况下为常数, 平均时间为二分之 n 的平方, 且其分布呈光滑的曲线, 并且这样的曲线很容易通过算例描绘出来. 在 n 等于任何值的时候, 都具有这样的特点.

NP 完全问题, 比如哈密尔顿环, 就完全不是这样了. 哈密尔顿环的特点是: 对一个不大的 n , 其可能的算例数量极其庞大, 且这些算例的难易程度分布相当复杂, 没有规律, 现在还没有人能掌握这些算例难易程度的分布规律. 例如, 国际某网站有关于最难算的哈密尔顿的算例, 这些算例用笔者的程序可以非常轻松和快速地解决. 因而, 对于某个 NP 完全问题, 一个计算程序所说在最坏情况下的计算时间, 只能指的是在所算的例子中最慢的那一个, 而不是指: 该程序找到了这样的例子, 它代表了此问题计算时间复杂度的上限. 这样的例子

是没有人能找得到的, 而冒泡排序之类的多项式问题则非常容易找到这样的例子, 且呈固定的概率分布.

故而对 NP 完全问题算法的思维不能停留在对一些简单问题的思维层面上. 就算真的能找到在最坏情况下的问题, 也不能排除在客观世界存在有这样的 NP 完全问题, 比如: 它的时间复杂度上限是某个值, 但在某个数据段, 最坏的情况的复杂度是另一个值, 在另一个数据段最坏的情况又是一个不同的值, 等等. 这就是为什么 NP 完全问题时间复杂度难以确定的根本原因.

自从史蒂文库克论证了 NP 完全问题的存在, NP 是否等于 P 随即开始困扰人类, 考量着人类复杂的思路能力和计算能力. 此问题也很快被公认为最具挑战性的世界难题. 如果能证明某个 NP 完全问题存在多项式时间算法, 即可判定所有 NP 问题都具有多项式时间算法. 如前所述, 迄今已发现 4 千多个 NP 完全问题, 还没有人能论证完全问题学者具有多项式时间算法, 也没有人能否定其具有多项式时间算法. 相关领域的学者往往根据自己的感觉或倾向拥有自己的判断, 这些判断不能说是科学的或有实际价值的.

有人对一些数学家和计算机科学家做过统计, 结果大多数倾向于认为 NP 不等于 P, 只有小部分认为两者相等.

一些科学家在提出 NP 不等于 P 的判断时, 所举的理由仅仅是泛泛的, 而不具备严格的科学认证价值. 举例如下:

一个算法学家, 在一本算法专著上写到: 迄今已出现了大量 NP 完全问题, 由于许多最优秀的算法专家和数学家在长期研究这些问题, 却没有找到一个多项式算法, 故倾向于判断 NP 不等于 P^[1].

ACM 期刊主编是这样论证 NP 不等于 P 的: 若谁证明了 NP 等于 P, 则他不仅只是解决了 NP 问题, 所有 7 大世纪难题他都解决了, 因为所有科学研究问题的解决都属 NP^[7].

还有专家认为: 由于非确定性图灵机的计算能力明显强于确定性图灵机, 从而 NP 不等于 P. 当然, 也有不少专家认为 NP 等于 P.

下面给出 NP 是否等于 P 的一些启发式思考.

3 科研问题的解决与 NP 完全问题

NP 问题为何如此具有影响力? 其原因一是问

题本身确实难解,极具挑战性,二是,它考量人类思维能力和计算能力的极限.人的思维是串行的而不具备并行思维能力,而所有科学问题的解决途径,其实都是 NP.

若是 NP 等于 P,则理论上,只具有串行思维能力的人类,可以解决所有科学难题.而若是 NP 不等于 P,也就是大量的 NP 问题会是指数型的,则不幸得很,大量科学问题人类思维很难解决.因为指数型通常意味着 2 的 n 次方或更大,当 n 的规模达到小小的 100 时,解决问题所需的思维步骤将达 100 万亿亿步,这是人类思维能力所无法企及的,哪怕花上万万年的时间.

从哲学上可以这么说,是否赞成 NP 等于 P,是区分可知论和不可知论的分水岭.

公认为 20 世纪最伟大的数学家的希尔伯特有句名言:我们必须知道,我们必能知道!可见,本质上,希尔伯特是赞成 NP 等于 P 的!

而他在 20 世纪刚开始所提出的 23 个高不可攀的数学问题,也已经陆续得到了解决,仿佛是在证明他的“我们必能知道”的断言.

人类历史上,一个个科学难题在不断被解决,难道不是在印证着 NP 等于 P 吗?

笔者对此的质疑逻辑是:如前所述,所有科研难题的解决途径是 NP,因而 NP 是否等于 P 这一难题的解决途径无疑也属 NP.鉴于这是科学难题,许多科学家判断,该问题人类长时期很难解决,例如上述 ACM 的期刊主编就是这样判断的,因而有理由认为该问题属于 NP 难,并且其解决过程所包含的参量也就是 n 不可能很小.

这意味着任何宣称证明了 NP 不等于 P 的人,其实是在用自己证明的结论,去否决自己证明的可能性和正确性,也就是说,是在循环否定.

4 围棋软件开发与 NP 完全问题

曾有人提议,若能开发一个围棋软件,能打败所有围棋高手,也就是说其思路已达到最优,那不就一切都证明了吗?此提议非常好,但要做好还有诸多困难,而且就算做好了,也不意味 NP 问题的解决.

下围棋属敌对搜索,是极大极小搜索加剪枝问题中的一种.问题在于,它的分支数非常大,也就是可选的点很多,因而计算深度就只能很浅了,否则计算量和储存量都会大得惊人.不仅如此,它的状态

值量化非常困难,从而在进行优劣选择以及剪枝时,非常难以把握.因此,迄今最好的围棋软件只能达到业余二段的水平,与专业高段棋手比当然是相差甚远.

人下围棋能达到专业强九段的水平,不妨假定此水平极高.由此就产生了如下问题:(1)围棋是 NP 吗?(2)围棋是 NPC 吗?(3)此问题能在多项式内解决吗?

注意到强九段,显然,不能认为强九段的思维能力和记忆能力能满足指数型.不妨设想人类能出现这样顶级的围棋高手,他下棋就能达到最优,也就是说能在多项式时间内完成判断计算.这就意味着,一个明显的指数型搜索问题,有人却可在多项式内完成.这是如何办到的呢?回答只能是:在充分研究后,加上充分的知识积累以及复杂的关联信息的充分把握.从逻辑上可以判断,人能做到的,软件也应能做到,且不会增加计算量和储存量.

对这个问题的分析,可以得到解决 NP 完全问题的某些启发.

此外,近年来一些论文提到的一些研究技巧,亦对 NP 问题的研究有所助益^[8-10].

针对 Hamilton 环这一 NP 完全问题的多项式时间算法的研究尝试也一直在进行^[11].多年来,笔者也坚持进行该问题的研究,已经有相当乐观的结果.

5 个体和群体及概率与 NP 完全问题

同样,从启发思维的角度,如前所述,至今已发现了 4 000 多个 NP 完全问题,且还会继续发现.由于任何一个 NP 完全问题,都可以多项式规约到另一个任意的 NP 完全问题,也就是说,所有 NP 完全问题两两之间的距离是多项式,这件事本身强烈地昭示着(strongly imply),NP 问题具有统一的求解规律和难解度,并且也应具有多项式量级.

客观世界的任何一个群体,其任意个体之间某个属性的差值,与个体属性的绝对值通常都处在同一个量级.举例说来:通常成人的体重是百斤量级,很肥壮和很瘦的人之间体重的差值也是百斤量级.同样,很肥大的蚂蚁与很瘦小的蚂蚁体重之差值也与通常单个成年蚂蚁的体重处在同一个数量级.

再举一个例子:假使在某个太空中随机选 n 个点, n 显著大于 1,若其中任两个点之间的距离都不超过 10^{10} 米,就有理由认为,该太空本身的最大尺

度也在 10^{10} 米量级.

不难看出,这些问题之间具有相同的内在逻辑,从而也给人们 NP 完全问题的认识上以启发.

6 结 语

NP 完全问题的相关概念十分的抽象,难以把握,无论学生或研究人员,常有相关问题的概念错误或理解模糊,本文用通俗的语言揭示了这些概念的本质.

在 NP 完全问题的研究中,最为关键的是正确的研究方向,若是研究方向为并不成立的谬误所误导,则不仅会导致多走弯路,甚至可能是完全做无用功. 其中一个最大的谬误就是,认为 NP 当然的不等于 P. 这就意味着所有 NP 完全问题不可能有多项式时间算法,因此从根本上限制了这方面的研究. 许多学者包括一些专家都将其作为限制框框. 这仅仅只是一些研究人员的一种个人倾向,而绝不是定论. 有理由认为其有可能甚至极可能是错的. 还有一种倾向就是将 P vs. NP 问题过分神秘化,要么宣称该问题不能在人类已有知识框架内解决,要么宣称今后很长时期人类不可能解决. 所有这些宣称并无切实的依据. 本文详细论述了 NP 完全问题的实质,并从多个角度,用启发式思维方式,分析了其时间复杂度及其特性,以及可行的研究前景和研究方向. 可供相关领域的学者参考.

致 谢

感谢湖北省自然科学基金对本研究的支持!

参考文献:

- [1] ARORA S, BARAK B. Complexity Theory: A Modern Approach Cambridge University Press [M]. Cambridge, 2009
- [2] AARONSON S. Is P versus NP formally independent [J]. Bulletin of the European Association for Theoretical Computer Science, 2003, 81(10): 109-136.
- [3] 杜丁柱,葛可一,王洁.计算复杂性导引[M].北京:高等教育出版社,2002:35-57.
DU ing-zhu, Ge Keyi, Wang Jie. Introduction to Computing Complexity [M]. Peking: High Education Press, 2002: 35-57. (in Chinese)
- [4] SARTAJ Sahni, Data Structures, Algorithms, and Applications in C++ [M]. McGraw-Hill, 1998.
- [5] COOK S A. The complexity of theorem proving procedures [M]. Proceedings of Third Annual ACM Symposium, New York: on Theory of Computing, Association for Computing Machinery, 1971: 151-158.
- [6] KARP R M. Reducibility among combinatorial problems [M]. Miller R E, Thatcher J W Plenum Press, Complexity of Computer Computations, New York: 1972: 85-104.
- [7] LANCE Fortnow. The Status of the P Versus NP Problem [J]. Communications of the ACM, 2010, 52(9): 78-86.
- [8] 朱丽君, 陈金芳. 大数据下中文期刊论文被引分析 [J]. 武汉工程大学学报, 2015, 37(5): 74-78.
ZHU Li-jun, CHEN Jin-fang. Citation analysis on Chinese Periodicals Under big data [J]. Journal of Wuhan Institute of Technology, 2015, 37(5): 74-78. (in Chinese)
- [9] 付 敏, 戴祖旭, 王道蓬. 压缩编码的上下文树构造算法 [J]. 武汉工程大学学报, 2015, 37(4): 51-55.
Fu Min, Dai Zuxue, WANG Dao-peng. Context tree algorithm based on compression encoding [J]. Journal of Wuhan Institute of Technology, 2015, 37(4): 51-55. (in Chinese)
- [10] 殷秀叶. 大数据环境下的相似重复记录检测方法 [J]. 武汉工程大学学报, 2014, 36(9): 66-69.
YIN Xiu ye. Method for detecting approximately duplicate database records in big data environment [J]. Journal of Wuhan Institute of Technology, 2014(9): 66-69. (in Chinese)
- [11] POSA L. Hamiltonian circuits in random graphs [J]. Discrete Math, 1976(14): 359-364.

NP-complete problem and its future

DU Li-zhi, CHEN He-ping, FU Hai-dong

College of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan 430065, China

Abstract: P versus NP is one of the most important problems in theoretical computer science. Because the concepts about it are very abstract and complicated, some scholars and students in computer science often misunderstand them. A lot of published papers contain these misunderstandings. The main problems are: the defaults in understanding the concepts of NP and NPC, unclearly understanding the concepts of deterministic turing machine and non-deterministic turing machine, misreading the relationship of P and NP and misleading in the study direction of NP, etc. Of all these concepts, the core concept is the NP-complete problem. In this paper, we analyzed the misunderstandings. By deeply studying the definitions, we revealed their essence. Specially, by analyzing a lot of questions in different fields, we gave some heuristic strain of thoughts for the possible ways to solve the NP-complete problem and the possible directions to study it.

Keywords: deterministic turing machine; nondeterministic turing machine; NP-complete problem

本文编辑:陈小平