

图灵 (Alan Turing) 的伟大贡献

-- 纪念图灵诞辰 100 周年

西北大学 郝克刚



英国数学家图灵 (Alan Turing) 是计算机和计算机科学的理论奠基人。他出生于 1912 年 6 月 23 日, 也就是说明年是他诞辰 100 周年。为了纪念他对计算机科学的伟大贡献, 从今年年底开始世界计算机界要举行一系列的纪念活动, 并称 2012 年是图灵年 (Alan Turing Year)。为了普及计算机科学的基本知识和弘扬科学精神, 特撰写此文, 列举并简要介绍图灵的一些重要贡献以资纪念。

就如同文学院的学生都熟悉曹雪芹和红楼梦一样, 学习计算机有关专业和学科的学生, 不能不知晓图灵和图灵机等的基本知识和概念。为此以同样的内容向大学生们做一次通俗的学术讲座。

以下是本文的内容和讲座的纲要, 放在博客上同大家共享。

- 1) 图灵的生平
- 2) 图灵机和通用图灵机
- 3) 通用电子计算机出现的理论基础
- 4) 有超越图灵机计算能力的模型吗
- 5) 对不可解问题的证明
- 6) 为计算机科学的研究奠定重要的理论基础
- 7) 图灵测试, 计算机的智能
- 8) 图灵奖, 中国人的期盼和展望

1) 图灵的生平

图灵 (全名 Alan Mathison Turing) 1912 年 6 月 23 日出生于英国伦敦近郊。父亲是英国在印度的一名官员，来回奔波。他小时没有同父母生活在一起，而是同哥哥住在一个退休的夫妇家中。中学寄宿，酷爱数学和科学，喜欢赛跑。

1930 年图灵进入剑桥大学 King's College 攻读数学。1934 年他 22 岁时，完成了学位论文，推广了冯·诺伊曼 (Von Neumann) 的群论模型。

1935 年图灵对数理逻辑发生兴趣。1936 年发表“论可计算数及其在判定问题中的应用”一文。文章的主题是回答希尔伯特 (David Hilbert) 在 1900 年提出的 23 个数学难题之一：是否所有的数学问题都是可解的？这涉及到逻辑系统的完备性。图灵机器就是为此提出的一个概念。论文发表后引起美国科学家的重视，应邀到美国普林斯顿大学，1938 取得博士学位。

1938 年回英国剑桥大学。1939 年进入英国政府的一研究机构，破译了德军密码，战后光荣受勋。战后进入英国国家物理实验室，开始了设计和建造英国的电子计算机工程 (ACE)，其中设计用到了存储程序的思想。1948 到曼彻斯特大学工作。

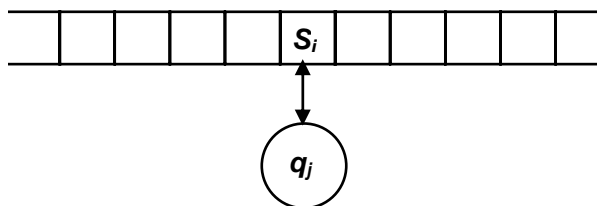
1951 被选为英国皇家学会院士。1952 年，因同性恋被法院传讯，指控“行为极端不当”。1954 年 6 月 7 日因吃了含氰化物的苹果，在家中死亡，享年不足 42 岁。死因成不解之谜。

2) 图灵机和通用图灵机

图灵机器是图灵在他的论文中提出的一个抽象的计算机模型。模型非常简单，由下面几部分构成：

n 个符号 $S=\{s_1, \dots, s_n\}$, 其中有空格符号 $b \in S$; m 个状态 $Q=\{q_1, \dots, q_m\}$, 其中有初始状态 $q_1 \in Q$

一条两个方向或一个方向是潜在无穷长的由格子组成的带子。每个格子可以存放一个符号。带子边附有一个读写头，读写头处于某个状态并指向某个格子，可以读写所指格子上的符号，并在带子上左右移动。



另有一组有穷个形如下式的规则：

$s_i, q_j \rightarrow s_k, q_l, d$. 其中 $d=H, L$ 或 R .

图灵机器这样执行：开始时，在图灵机带子的一串格子上放上由符号 (除 b 外) 组成的初始字，其余格子均放置空格符号 b 。读写头处于初始状态 q_1 ，并指向初始字的第一个格子。然后如下执行。如果所指的符号是 s_i ，读头的状态是 q_j ，刚好是某规则的左端，则按照该规则做动作：在所指格子上写符号 s_k ，读头变换状态为 q_l ，根据 d 的值 ($d=H, L$ 或 R) 读头位置保持不动 (H)，左移 (L) 或右移 (R) 一格。

上一步做完后，如果所指的符号和读头的状态刚好又是规则组中某规则的左端，则图灵机器按此规则继续执行。余类推，直到所指的符号和读头的状态不能同所有规则的左端匹配时，图灵机停机，执行终止。一般将执行终止时带子上的字作为相对于初始字的计算结果。

我用 Java 编了一个图灵机的模拟软件，在讲座时可以演示图灵机的执行过程。如果阅读此文就只好自己做做练习，来体验图灵机的执行了。例如下面就是一个把二进制数展开成

同等数量的 1 的图灵机。例如, 初始字是 10, 结果就是 11, 初始字是 101, 结果就是 11111 等, …。此图灵机的符号集= $\{b, 0, 1\}$, 状态集= $\{q_1, \dots, q_7, St, Er\}$, 规则集合是:

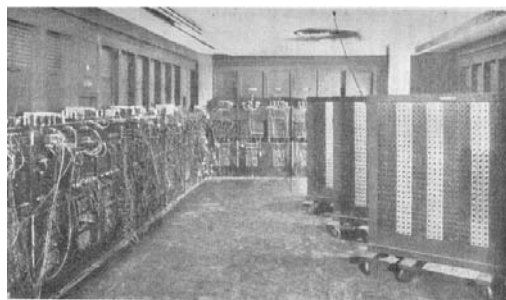
$b, q_1 \rightarrow b, q_7, L;$ $b, q_2 \rightarrow b, q_3, R;$ $b, q_3 \rightarrow 1, q_4, L;$ $b, q_4 \rightarrow b, q_5, L;$
 $b, q_5 \rightarrow b, Er, H;$ $b, q_6 \rightarrow b, q_1, R;$ $b, q_7 \rightarrow b, St, H;$
 $0, q_1 \rightarrow 0, q_1, R;$ $0, q_2 \rightarrow 0, q_2, R;$ $0, q_3 \rightarrow 0, q_3, R;$ $0, q_4 \rightarrow 0, q_4, L;$
 $0, q_5 \rightarrow 1, q_5, L;$ $0, q_6 \rightarrow 0, q_6, L;$ $0, q_7 \rightarrow b, q_7, L;$
 $1, q_1 \rightarrow 1, q_2, R;$ $1, q_2 \rightarrow 1, q_2, R;$ $1, q_3 \rightarrow 1, q_3, R;$ $1, q_4 \rightarrow 1, q_4, L;$
 $1, q_5 \rightarrow 0, q_6, L;$ $1, q_6 \rightarrow 1, q_6, L;$ $1, q_7 \rightarrow 1, Er, H;$

如果执行中每次只可能有一个规则匹配, 也就是说所有规则的左端都不完全相同, 图灵机的执行是唯一确定的, 称这样的机器为确定的图灵机。反之, 有两个或更多的规则的左端完全相同时, 图灵机的执行就不是唯一确定的, 称这样的机器为非确定的图灵机。

图灵的伟大贡献不仅是提出了图灵机器的概念, 更重要的是还提出了通用图灵机 (Universal Turing Machine) 的概念。可以证明存在着一个这样的图灵机 T, 称为通用图灵机: 对任给的图灵机 A, 只要把它(A)的规则和初始字, 并列起来作为通用图灵机 T 的初始字, 让通用图灵机 T 运行, 运行结果就是图灵机 A 的运行结果。而正是这个思想奠定了 10 年后通用电子计算机出现的理论基础。

3) 通用电子计算机出现的理论基础

以前的资料认为最早电子数字计算机是 ENIAC (Electronic Numerical Integrator and Computer), 1946.2 诞生于美国宾州大学莫尔学院。ENIAC 是一台为各种炮火计算弹道的专用计算机, 程序用外接电路板输入。后查证, 实际上世界上第一台专用电子计算机是 1939 年爱荷华 (Iowa) 州立大学开发的 Atanasoff -Berry Computer(简称 ABC)。此外, 后来还发现二战期间德国当时也秘密研制成功了计算机。



1945 年冯·诺伊曼发表了“关于离散变量自动电子计算机 EDVAC (Electronic Discrete Variable Automatic Computer) 的设计草案”。这台计算机由他设计, 不仅数据, 程序也可存储在计算机中。数据可变, 程序也可变, 是所谓“存储程序式”的通用计算机。建造合同 1946 年 4 月签订。预算是十万美元, 但最后耗资五十万。1949 年 8 月交付美国军队的弹道研究实验室, 1951 年开始运行

最先实现“存储程序式”计算机的是 EDSAC(Electronic Delay Storage Automatic Calculator)。它采用水银延迟先做存储器, 可存储 512 个 34bit 字长的字, 研制者是英国剑桥大学威尔克斯(M.V.Wilkes)。伦敦一家面包公司(Lyons)投资, 1949 年 5 月 6 日试运行成功。1951 年批量生产投入市场 LEO(Lyons Electronic Office)。但是他的设计思想完全来自冯·诺伊曼的 EDVAC 的设计。而冯·诺伊曼的设计思想却又来自图灵 1936 年的文章中引入的概念—图灵机器和通用图灵机。

之所以这么快就由硬件连线构成的专用计算机过渡到“存储程序式”的通用计算机, 完全归功于通用图灵机概念的引入。因而我们说, 是图灵的图灵机理论奠定了通用电子计算机设计的理论基础。这种理论准备同电子技术的结合才最终产生了 20 世纪最伟大的奇迹。

4) 有超越图灵机计算能力的模型吗

图灵机是为直观的“计算”给出一个严格的形式化的定义。它的神妙之处还在于它的组成和执行规则相当简单,但是功能却非常强大。试图对其扩展来扩大它的计算能力都不成功。例如多增加几个无穷长的带子和读头,最后证明它的计算能力还是等价于原来的图灵机。即使是非确定的图灵机的能力也等价于确定的图灵机。

图灵 1937 年被邀请到美国普林斯顿和丘奇(Alonzo Church)一起合作,他们提出了一个后来被叫做丘奇-图灵论题。这个论题断言图灵机同直观的有效的函数计算具有等价的问题求解机制。即所有“能解”的问题都存在一个图灵机,只要把问题放在图灵机带子上,若有解则停机后带子内容即是解答。这个断言叫做“论题”是由于他无法严格证明。

那个时代和后来曾经提出过不少的形式化计算模型,如λ演算、递归函数、正规算法、POST 系统、递归算法(胡世华)等,全都被证明同图灵机等价。这些事实一定程度上加强了这个论题。

当然在学界也有一些对此论题的质疑,例如有人认为交互式机器超越了图灵机(Peter Wegner),有人认为量子计算机,生物计算机可能会超越图灵机,但是这些意见都还没有能给出具有说服力的论证,从而也没有为普遍学者所认可。在纪念图灵诞辰 100 周年之际,关于是否有超越图灵机计算能力的模型也是一个争论的热门话题。

5) 使不可解问题的证明成为可能

由于图灵机是为“计算”给出的一个严格的形式化的定义。从而使严格证明某些问题是“不可计算”(“不可解”或“不可判定”)成为可能。要知道这种否定的证明通常是相当困难的,所以说这也是图灵的一个重要贡献。

首先可以证明图灵机的停机问题是不可判定的。接着证明了推导系统的字的问题是不可判定的。后来又证明了逻辑系统以外的许多实际数学问题是不可判定的。如有名的希尔伯特第十问题是不可解的,即不存在这样的算法,它能判定一个任意的丢番图方程(Diophantine Equation)是否有整数解。

即使是不可解的问题,也有程度层次的不同,克林(Stephen Kleene)曾对其进行了分层。笔者早期也曾涉及此类研究,提出过“可构造实数论中若干谓词在 Kleene 分层下所属的类型”(《数学学报》1964 年第四期。)



6) 为计算机科学研究奠定重要的理论基础

图灵机的提出,影响深远,可以说它为以后整个计算机科学研究奠定了重要的理论基础。例如关于形式语言和自动机的理论研究就以图灵机作为基础,它对计算机编译系统和操作系统技术的发展起着重要作用。

乔姆斯基(Avram Noam Chomsky)曾按生成文法的不同对语言进行分类。所谓语言就

是某字母表上字的集合。而后来发现语言又和接受它的机器类型有关。说某机器 M 接受某个字 w ，是指如果以字 w 作为机器 M 的输入（对图灵机来说就是作为他的初始字），运行后以某指定的接受状态结束计算。也就是说，如果 M 在其他状态结束计算，或计算不终止，则 M 不接受该字 w 。

理论研究证明语言，生成文法和机器的类型有如下的对应关系：

语言类型	生成文法	接受的机器类型
0 型语言	0 型文法	图灵机
一型语言	上下文有感文法	线性有界自动机
二型语言	上下文无关文法	下推自动机
三型语言	正则文法	有穷自动机

再例如关于算法复杂度的研究，也常以图灵机作为研究的起始模型。我们知道，同样是算法，在机器上运行时所需要的时间和空间资源的数量时常相差很大。因而需要定义算法的复杂度来作为度量算法优劣的一个重要指标。假定算法在图灵机上计算的输入字的长度是 l ，那么完成此计算所需要的最长时间（即运算的最长步数）是 l 的一个函数，称此函数为此算法的时间复杂度。同样，完成此计算所需要的最大空间（即运算涉及的格子最大数量）也是 l 的一个函数，称此函数为此算法的空间复杂度。例如函数不超过多项式函数，就说此算法具有多项式时间或多项式空间复杂度。函数不超过指数函数，就说此算法具有指数时间或指数空间复杂度。

大家知道指数函数要比多项式函数增长得快得多，因而常认为具有多项式时间复杂度的算法是“实际可行的 (feasible)”算法。而具有指数时间复杂度的算法是实际不可行的。

例如：多项式函数 $t=n^3$, $n=60$, $t=216000$ ，一台百万次计算机，0.2 秒即可完成。而指数函数 $t=3^n$, $n=60$, $t=3^{60} \sim 4 \times 10^{28}$ ，若能用 10 亿台百万次计算机并行运算，需要运行一百万年。

这里再顺便介绍一下悬赏奖金一百万美元巨奖，被称为“千僖年数学难题”之一的“P = NP?”问题。这个问题是：“在多项式时间界限下，确定的和非确定的图灵机器是否具有同等的功能？”

我们知道，确定的和非确定的有穷自动机的功能是相同的，它们所接受的语言都是正则集合。如果不加多项式时间的限制，确定的和非确定的图灵机的功能也是相同的，它们所接受的语言都是递归可枚举集。如果对图灵机加上空间的限制，在多项式空间界限下，确定的和非确定的图灵机也具有同样的功能。但是，并不是在所有情况下确定的和非确定的机器都具有同样的功能。例如，对具有一个下推存贮的有穷机器来讲两者的功能是不相同的，非确定性的下推自动机所接受的语言是上下文无关语言，而确定的下推自动机所接受的语言却是上下文无关语言的一个真正的子类。

那么在多项式时间界限下，确定的和非确定的图灵机器是否具有同等的功能呢？即是否 $P = NP$ ？回答究竟是肯定还是否定，只能有一种。这个问题的提法相当清晰，但是要解答这个问题却不容易。当代很多有名的计算机科学家都研究过这个问题，问题至今仍未解决，而且愈来愈觉得是相当困难的。解决这个问题似乎需要在方法上有重大突破。

上世纪 70 年代提出的 NP 完全的理论，对解决此问题有很大的推进，但仍未最终解决。笔者 30 年前曾写过一篇综述文章，“NP 完全问题及有关理论研究”（《计算机科学》，1980 年 1 期。）

不久前，有一位 HP 公司的工程师宣称他证明了 $P \neq NP$ ，不过目前还尚未被认可。

7) 图灵测试, 计算机的智能

电子计算机诞生以后, 人们惊奇地发现它的能力大大超出原来的预期。计算机不仅可以做大量的计算, 还能进行复杂的推理。于是就把它同人的大脑进行比较, 提出“计算机能思维吗”的问题。这里涉及到对“什么是思维”的理解和界定, 涉及哲学、认知学以及社会学等各个方面, 相当复杂众说纷纭, 很难有一个统一的标准。图灵 1950 年 10 月在英国曼彻斯特大学发表论文“计算机和智能”, 巧妙地把这个问题转化为一种可操作的方法, 那就是测试。后来被称为图灵测试。简单说就是与其争论什么是“思维”, 不如我们去做实验测试。通过了测试就叫计算机能思维, 否则就说还达不到思维的水平。

图灵测试是这样设计的。测试分测试人员和被测试方两部分。被测试方由 A 和 B 构成, A 和 B 分别是一个人和一台被测试的计算机。测试人员和被测试方是分开的, 提问和回答是通过一些中间设备实现的。测试人员并不知道 A 和 B 那个是人那个是计算机。测试时由测试人员分别向 A 和 B 提问, 由被测试的人或者计算机回答问题。通过一系列的提问后, 如果测试人员能够通过问题的回答, 正确地分出 A 和 B 谁是人谁是机器, 说明计算机还没有达到人的水平, 那机器就没有通过图灵测试, 如果测试人分不出 A 和 B 谁是机器谁是人, 那这个机器就通过图灵测试。图灵指出: “如果机器在某些条件下, 能够非常好地模仿人回答问题, 以至提问者在相当长时间里误认它不是机器, 那么机器就可以被认为是能够思维的。”

当时的计算机根本无法通过这一测试。图灵预言, 50 年内, 即在 20 世纪末会有计算机通过图灵测试。图灵测试没有规定问题的范围和提问的标准, 如果想要制造出能通过试验的机器, 必须在电脑中储存人类所有可以想到的问题, 储存对这些问题所有合乎常理的回答, 并且还需要理智地作出选择。这几乎是不可能的。到目前为止还没有电脑能通过图灵测试。但是如果限制在一定的领域和范围之内通过图灵测试是完全有可能的。

人工智能专家经过多年的努力, 开发了不少智能软件, 在理论和实践上取得了很大的进步。1997 年 5 月 3-11 日, IBM 的计算机深蓝 (Deep Blue) 以 2 胜 1 负 3 平的成绩第一次战胜国际象棋冠军卡斯帕罗夫大师。在世界引起轰动。也可以说在一定意义下实现了图灵的预言。

自然对于图灵测试的理解以及它的作用等方面, 学界也有各种不同的争论。而正是由于有这些争论才推动了科学技术的发展。



8) 图灵奖, 中国人的期盼和展望

1966 年, 美国的国际计算机学会 ACM (Association for Computing Machinery) 为表彰图灵对计算机科学的伟大贡献, 设立了图灵奖 (A. M. Turing Award), 每年一届, 奖金 25 万美元, 用以奖励在计算机科学研究中做出创造性贡献, 推动计算机科学技术发展的杰出科学家。选择条件要求很高, 程序极严, 一直被公认为是世界计算机科学领域的最高荣誉奖项, 相当于计算机科学界的诺贝尔奖。奖金由 Intel 和 Google 公司提供。

1966-2010 年已举行 45 届, 有 55 名科学家获此殊荣。许多著名的对计算机科学技术作出重大贡献的科学家都是图灵奖的得主。获奖者的名单和他们一个个的贡献推介, 活生生地

展现了几十年来计算机科学技术发展的历程和辉煌成就的方方面面。

令我们中国人感到遗憾的是我们国内培养成长的专家至今还没有一个在获奖名单中出现。获图灵奖的唯一一位华人是 2000 年得主姚期智博士(Chi-Chih Yao)，台湾大学毕业，在美国哈佛大学和伊利诺斯大学取得博士学位，曾在美国著名的麻省理工学院、斯坦福大学、加州大学贝克莱分校任教，获奖时任美国普林斯顿大学教授。现在海归聘为中国清华大学教授。

很多人都在问和思考一个问题：为什么我们培养不出高水平的能获得诺贝尔奖和图灵奖的科学家？我认为除了我们的大学和研究所的研究水平、研究环境与先进国家有较大的差距外，可能在我国的教育制度和科研体制上有缺陷，不利于一流人才的成长。从思想氛围上过于浮躁，鼓励和导向倾向于急功近利。研究人员思想上整天考虑的是如何去完成论文数量任务，如何去申请科研项目经费，如何去通过鉴定验收，如何去争取获奖，如何去拼一级一级的职称。那里有时间和精力去思考真正的自己感兴趣的研究问题，谁还敢冒出不来成果坐冷板凳的风险去研究重要但很难的大问题，结果就导致研究上的“短平快”低水平重复，垃圾论文滥竽充数，甚至弄虚作假、侵权抄袭丑闻百出。

我们国家的科学研究水平同国家的经济和政治地位是不匹配的。大家都看到了这点，都有殷切的期待和展望，希望在不远的将来能够有我们自己培养的科学家做出重大的贡献。其实有很多外国学者也这么看。例如 1993 年图灵奖得主世界著名计算机科学家米勒 (Robin Milner) 在他的经典著作“通信与移动系统： π -演算”中译本 (2009 年出版) 序言中，对中国学者就给与了很大的期待，他写道：“中国，作为在世界上发挥日益重要作用的大国，具有引领为新技术建立科学基础的机会……。”

这也正是我们广大中国学者所日夜期盼的，外国人说出了我们中国人的心声。我们希望把机会变为现实。



(全文完) 2011 年 9 月 19 日

作者简介：郝克刚。 西北大学信息科学与技术学院教授。早年从师于中国科学院已故著名的数理逻辑学家，计算机科学家胡世华、唐稚松院士。曾在美国马里兰大学计算机科学系作访问学者。中国计算机学会 Petri 网专委会资深委员。研究领域：软件工程及相关理论。