上世纪 (数理) 逻辑的一些重要结果简介

哲学数学计算机中的逻辑课程 (2016 年秋)

王彦晶
北大哲学系

2016 年 12 月 29 日

本节课的内容: 不可能完成的任务

- 图灵机与铺砖 (Tiling)
- 图灵停机问题 (Halting problem)
- 一阶逻辑不可判定性 (Undecidability)
- 康托定理, 罗素悖论与对角线方法 (Diagonalization)
- 公理集合论及连续统假设 (Continuum Hypothesis)
- 哥德尔第一不完全性定理
- 哥德尔第二不完全性定理

具体图灵机的例子 (自己试试看)

https://turingmachinesimulator.com/

图灵机与铺砖

王的砖块 (Wang tiles), 王浩的贡献之一.

判断任给有穷多种四色砖块是不是铺满整个平面. 存不存在有穷多个砖块能铺满平面但是只能是非周期性的 (确实存在).

用铺砖可以刻画图灵机及纸带状态在时间上的展开.

二进制加 1 的图灵机 (from Peter van Emde Boas)

- $Q = \{q, r, h\}$ (h 是停机状态)
- $\Sigma = \{0, 1, B\}$ B 表示空字符
- 指令集如下:
  $(q, 0, q, 0, R)$,
  $(q, 1, q, 1, R)$,
  (q, B, r, B, L),
  $(r, 0, h, 1, S)$,
  $(r, 1, r, 0, L)$
  $(r, B, h, 1, S)$, 这里 S 代表不动.

每一行表示纸带以及读写头的情况 (如第一行的 $q0$ 表示读写头停在纸带最左边读到 0, 内部状态为 q)

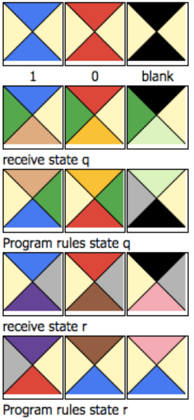
q0	1	0	1	1	B
0	q1	0	1	1	B
0	1	q0	1	1	B
0	1	0	q1	1	B
0	1	0	1	q1	B
0	1	0	1	1	qB
0	1	0	1	r1	B
0	1	0	r1	0	B
0	1	r0	0	0	B
0	1	h1	0	0	B

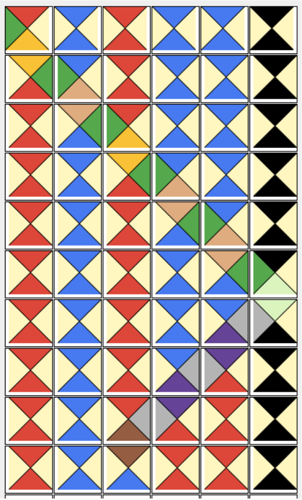
实现 $11(2^3 \cdot 1 + 2^2 \cdot 0 + 2^1 \cdot 1 + 2^0 \cdot 1)$ 的二进制表示再加 1 的过程.

这个过程可以用铺砖拼图表示

试试这里的游戏 (要保证相邻两个砖块相接的颜色一致):

http://www.squaringthecircles.com/turingtiles/





设计不同种类的砖块

- 第一类砖块 (symbol passing tiles) 负责上下 “传递” 纸带上的符号, 

- 第二类砖块 (instruction tiles) 代表指令集, . 例如, 淡咖啡色可以用来表示目前状态是 q 并且读到 1, 蓝色代表纸带上的符号 1, 绿色代表 q, 这样上面最左边的砖块可以用来表示指令 $(q, 1, q, 1, R)$, 这需要与下面第三种砖块配合使用.
- 第三类砖块 (receiving tiles) 负责与第二类砖块配合改变读写头位置与状态, , 例如, 上面提到的最左边的第二类砖块与第三类的中间的砖块可以左右拼接一起实现读写头往右移动一格并读到 0(红色), 这时用黄色表示目前状态是 q 并且读到 0.

图灵停机问题

有的图灵机里也可以运行其他 (作为输入的) 图灵机 (就像电脑里可以运行其他操作系统的虚拟机软件). 用 $\ulcorner M \urcorner$ 表示图灵机 M 可以被用来输入到虚拟机的 “源代码” (可用自然数去编码 M 的有穷指令).

停机问题: 任给一个图灵机 (的源代码), 任给一个输入, 判定这个图灵机是否能在有穷多步停下来.

假设存在这样一个图灵机 H, 能在有穷多步内判定任给的一个图灵机 M 在任给的一个输入 x 下能不能停机, 试图推出矛盾.

- $H(\ulcorner M \urcorner, x) = 1$, 如果 M 在输入 x 时停机, 否则令其为 0.
- 构造 $D(x)$ 使得 $D(\ulcorner M \urcorner) = H(\ulcorner M \urcorner, \ulcorner M \urcorner)$
- 构造 $T(x)$ 使得如果 $D(\ulcorner M \urcorner) = 0$ 则 $T(\ulcorner M \urcorner)$ 停机, 否则不停机
- 可是这样的话 $T(\ulcorner T \urcorner)$ 停不停机?
    - 如果停机则 $D(\ulcorner T \urcorner) = 0$ 即 $T(\ulcorner T \urcorner)$ 不停机
    - 如果不停机 $D(\ulcorner T \urcorner) = 1$ 即 $T(\ulcorner T \urcorner)$ 停机
    - 都矛盾!

一阶逻辑不可判定性

Berger (1966): 给定一个有穷的砖块类别集, 看是否能在一个平面里铺满砖块,可以证明: 一个图灵机不停机 iff 相应砖块集铺满整个平面. 这样如果有判定任何有穷砖块类别集是不是能铺满平面的办法, 也就有判断任意图灵机是否停机的办法了.

可以用一个 (包含一定符号的) 一阶逻辑公式描述这样的铺砖问题, 使得这个公式可满足iff 存在这样的铺砖.

例如可以用一阶逻辑说: 只有几种砖块, 任意两个相邻的砖块的相接的颜色是一样的, 每个砖块上下左右都有相邻的砖块.

所以 (包含一定符号的) 一阶逻辑语言的公式的可满足性 (及有效性) 问题不可判定. 当然可以直接把一阶逻辑公式的判定性问题划归到图灵停机问题上 (原始证明).

不同的铺砖问题对应不同的计算复杂度: bounded tiling, corridor tiling... 在研究不同逻辑的计算性的时候很好用.

康托定理和对角线方法

无穷是有大小的! 两个无穷集合可以比大小 (元素的 “多少”): 如果存在双射就一边大, X 到 Y 存在单射但不存在双射则 X 的基数 (Cardinality) 小于 Y 的基数, 记为 $|X| < |Y|$.

- 希尔伯特旅馆: 自然数那么多个房间, 再来个人也没关系 (大家都往下一个房间挪一挪) 所以全体自然数的集合和全体自然数再加一个数的集合一样大
- 奇数和与全体自然数 “一样多”
- 整数, 有理数和自然数 “一样多”

有没有比自然数多的?

实数比自然数多!

首先看 $\mathbb{N}$ 及其幂集的比较.

康托定理和对角线方法

假设如果 $|\mathbb{N}| = |\mathcal{P}(\mathbb{N})|$ 一样多, 则我们可以把自然数的子集一个个数出来 (记为 S_k):

	0	1	2	3	...
S_0	0	0	0	0	...
S_1	1	1	1	1	...
S_2	1	0	1	0	...
S_3	0	1	0	1	...
...	...	...	...	...	

每一行表示哪些自然数在 S_k 这个集合里: 在里面写 1, 不在写 0.

把对角线上的 0 和 1 互换, 也得到一个集合 (写 1 的那些自然熟的集合), 但是这个集合与 S_k 都不一样!

更一般的, 我们可以用这种思想证明 $|X| < |\mathcal{P}(X)|$ (康托定理), 本质上要证明不存在 X 到 $\mathcal{P}(X)$ 的满射.

图灵停机问题: 对角线的看法

假设有这样的图灵机 H, 对输入 $\ulcorner M \urcorner$ 和 x, 若停机写 1, 不停机写 0.

H 对应的输入输出表格为:

	$\ulcorner M_0 \urcorner$	$\ulcorner M_1 \urcorner$	$\ulcorner M_2 \urcorner$	$\ulcorner M_3 \urcorner$	...
$\ulcorner M_0 \urcorner$	0	0	0	0	...
$\ulcorner M_1 \urcorner$	1	1	1	1	...
$\ulcorner M_2 \urcorner$	1	0	1	0	...
$\ulcorner M_3 \urcorner$	0	1	0	1	...
...	...	...	...	...	

基于 H 定义一个新的图灵机 T, 使得对角线上有 0 则停机 (比如输出 0), 对角线上有 1 则让它不停机.

那么 $T(\ulcorner T \urcorner)$ 到底停不停?

有一个小镇上有一个理发师, 他给且只给不给自己理发的人理发, 请问他给不给自己理发?

定义 $R = \{x \mid x \notin x\}$, 请问 R 是否属于 R? 表示一个集合是否属于另一个集合的表格 (如 $X \in Y$ 就在相应的位置写 1):

$$
\begin{array}{cccccc}
 & ... & X & ... & Y & ... \\
\cdots & ... & ... & ... & ... & ... \\
X & ... & 0 & ... & 1 & ... \\
\cdots & ... & ... & ... & ... & ... \\
Y & ... & 0 & ... & 0 & ... \\
... & ... & ... & ... & ... &
\end{array}
$$

收集 “对角线” 上为 0 的集合构成一个集合 R (反转 0 和 1), 问这个表中 R 的对角线位置填啥? 有矛盾. 如果集合都不包含自己, 那 R 是所有集合的集合, 上面的证明显示所有集合的集合不应该也是集合!

不能乱定义集合! 用一阶逻辑的公式 (带二元谓词 $\in$) 来精确表示关于集合的推理规则! Zemelo-Frankle 再加 Axiom of Choice (AC):

Extensionality	$\forall x \forall y(x \approx y \leftrightarrow \forall z(z \in x \leftrightarrow z \in y))$
Paring	$\forall x \forall y \exists z \forall w(w \in z \leftrightarrow w \approx x \vee w \approx y)$
Union	$\forall x \exists y \forall z(z \in y \leftrightarrow \exists w(w \in x \wedge z \in w))$
Empty set	$\exists x \forall y(\neg y \in x)$
Infinity	$\exists x(\emptyset \in x \wedge \forall y(y \in X \to y \cup \{y\} \in x))$
Power set	$\forall x \exists y \forall z(z \in y \leftrightarrow \forall w(w \in z \to w \in x))$
Replacement	$\forall x \in y \exists ! z R(x, z) \to \exists w \forall v(v \in w \leftrightarrow \exists x(x \in y \wedge R(x, v))$
Regularity	$\forall x(\neg x \approx \emptyset \to \exists y \in x(x \cap y \approx \emptyset))$
Choice	$\forall x((\neg \emptyset \in x \wedge \forall y, z \in x(\neg y \approx z \to y \cap z \approx \emptyset))$
	$\to \exists y \forall z \in x \exists ! w \in z(z \in y)))$

$\exists!$(表示存在唯一), $\cup$, $\cap$, $\emptyset$, $\{y\}$ 皆可定义.

独立性结果

选择公理 (Axiom of Choice) 更易接受的直观描述: 任给一个集合, 存在一个函数把每个 A 的非空子集都挑一个元素出来.

让 Cantor 抓狂的连续统假设: $|\mathbb{N}|$ 与 $|\mathcal{P}(\mathbb{N})|$ 之间没有其他基数了, 或者说 $\mathcal{P}(\mathbb{N})$ 是第二小的无穷基数.

哥德尔 +Paul Cohen 的独立性结果

- ZF 如果是一致的, 则 ZF 推不出选择公理或其否定
- ZFC 如果是一致的, 则 ZFC 推不出连续统假设或其否定

其他的数学基础: ELEMENTARY THEORY OF THE CATEGORY OF SETS (LAWVERE)

什么都是集合.... π, e 也是集合? e 是与 π 的交是啥? 似乎没有本质的数学意义. 范畴论出发的 ETCS 的公理的思想:

1. Composition of functions is associative and has identities
2. There is a set with exactly one element
3. There is a set with no elements
4. A function is determined by its effect on elements
5. Given sets X and Y, form their cartesian product $X \times Y$
6. Given sets X and Y, form the set of functions from X to Y
7. Given $f : X \to Y$ and $y \in Y$, form the inverse image $f^{-1}(y)$
8. The subsets of a set X correspond to the functions from X to $\{0, 1\}$
9. The natural numbers form a set
10. Every surjection has a right inverse

哥德尔不完全性定理

一阶皮亚诺算术的理论 (PA 在一阶逻辑推理系统的基础上包括表达如下意思的公理:

- 0 不是任何数的后继
- x, y 的后继等则 x=y
- 加法乘法相对于后继的定义
- 归纳法的公理模式

第一定理 如果 PA 无矛盾, 那么算术语言中存在某语句, 使得它和它的否定从一阶皮亚诺公理出发都不可证 (甚至加强系统也没用). 想法: 用算术编码公式写出 "我不可证" 这样的句子, 利用对角线思想证明这句子和其否定都证不出来.

第二定理 若 PA 无矛盾, 那么它自己无法证明它的一致性 (甚至加强系统也没用).

- 逻辑在人类历史上与哲学, 数学, 计算机都有很深刻的联系
- 目前还有很多现实的作用 (特别是在计算机领域)
- 是一个反思性的学科, 关心元理论和否定性结果 (不可定义, 不可证, 不可判定, 不可完全等等)

你认为逻辑学是什么?

欢迎大家关注我们的其他课程

http://www.phil.pku.edu.cn/cllct/courses.php

下学期欢迎来上我的 “高级模态逻辑”.

谢谢大家!