上海师范大学 Shanghai Normal University

# 《离散数学》

## 8-函数 (Function)

杨启哲

上海师范大学信机学院计算机系

2024 年 9 月 16 日

上海师范大学 Shanghai Normal University

## 主要内容

- 函数的基本概念
- 集合基数
- 可计算性理论简介



## 函数的基本概念

上海师范大学 Shanghai Normal University

## 什么是函数?

我们已经接触到各式各样的函数，比如:

- $f(x) = x^2 + 1$
- $f(x) = \sin x + \cos 2x$
- $f(x) = \frac{1}{1+e^{-x}}$
- $f(x) = \begin{cases} 1, & x \in \mathbb{Q} \\ 0, & x \notin \mathbb{Q} \end{cases}$

可以看到，这些函数其实反映了 $x$ 与 $y$ 的某种关系，现在我们从关系的角度来给出函数的定义。

## 函数的定义



**定义 1** **[函数].**
令 $f$ 是一个 $A$ 到 $B$ 的二元关系，若 $\mathrm{dom}(f) = A$ 并且对于任意 $x \in \mathrm{dom}(f)$。存在唯一的 $y \in \mathrm{ran}(f)$ 使得 $(x, y) \in f$，则称 $f$ 是 $A$ 到 $B$ 的函数（映射），记作 $f : A \to B$。$xfy$ 也被记作 $y = f(x)$，并称 $y$ 为 $f$ 在 $x$ 的值。

**例 2.**
1. $f_1 = \{(x_1, y_1), (x_2, y_2), (x_3, y_1)\}$ 是一个函数。
2. $f_2 = \{(x_1, y_1), (x_2, y_2), (x_3, y_1), (x_1, y_2)\}$ 不是一个函数。

**补充说明**
1. 上述定义对多元函数也是符合的，因为 $x$ 可以理解成一个 $n$ 元组。
2. 如果 $\mathrm{dom}(f) \subset A$，则称 $f$ 是 $A$ 到 $B$ 的部分函数 (Partial Function)。



## 函数相等



由上述可知，一个函数可以看成一个集合，因此两个函数相等可以视作两个集合相等。

**定义 3** **[函数相等].**
令 $F, G$ 是函数，则 $F = G \Leftrightarrow F \subseteq G \wedge G \subseteq F$，即若 $F = G$ 则我们有：
1. $\mathrm{dom}(F) = \mathrm{dom}(G)$
2. $\forall x \in \mathrm{dom}(F)$，$F(x) = G(x)$

**例 4.**
1. 函数 $f(x) = x - 1$ 和 $f(x) = \frac{x^2-1}{x+1}$ 是不相等的。
2. 函数 $f(x) = \sin(\frac{\pi}{2} - 2x)$ 与函数 $g(x) = \cos 2x$ 是相等的。



## 一些其他的概念



- 像：令函数 $f : A \to B$，$A_1 \subseteq A$，则 $f(A_1) = \{f(x) \mid x \in A_1\}$ 称为 $A_1$ 在 $f$ 下的像。
- 完全原像：令函数 $f : A \to B$，$B_1 \subseteq B$，则 $f^{-1}(B_1) = \{x \mid x \in A \wedge f(x) \in B_1\}$ 称为 $B_1$ 在 $f$ 下的完全原像。
- 函数集合 $B^A$：令 $B^A$ 表示所有从 $A$ 到 $B$ 的函数的集合。

**例 5.**
令 $A = \{1, 2, 3\}, B = \{a, b\}$，$f = \{(1, a), (2, a).(3, b)\}$，$A_1 = \{1, 2\}$，$B_1 = \{a\}$，则：
1. $f$ 在 $A_1$ 下的像为 $f(A_1) = \{a\}$.
2. $f$ 在 $B_1$ 下的完全原像为 $f^{-1}(B_1) = \{1, 2\}$.
3. $B^A = \{f_0, \ldots f_7\}$，这里 $f_0 \sim f_7$ 代表 $A$ 到 $B$ 的不同的 8 个函数。



## 一些特殊的函数 (I)



- 常值函数：设 $f : A \to B$，如果存在 $c \in B$ 使得对所有的 $x \in A$，都有 $f(x) = c$，即 $f(A) = \{c\}$，则称 $f$ 是常值函数。
- 恒等函数：集合 $A$ 上的恒等关系 $I_A$ 被称作恒等函数，即对于任意的 $x \in A$，都有 $I_A(x) = x$。
- 特征函数：令 $A$ 是集合，对于 $A' \subseteq A$。定义 $A$ 上的特征函数 $\chi_{A'}$ 为：

$$\chi_{A'}(x) = \begin{cases} 1, & x \in A' \\ 0, & x \notin A' \end{cases}$$

## 一些特殊的函数 (II)



- $n$ 元运算：我们将函数 $f: A^n \to A$ 称为 $A$ 上的 $n$ 元运算。
  - $f(x,y) = x+y$，$f(x,y,z) = x+y\cdot z$ 定义了 $A$ 上的二元运算和三元运算。
- 单调函数：令 $(A, \leqslant_A), (B, \leqslant_B)$ 是一个偏序集，$f: A \to B$:
  - 如果对于任意的 $x, y \in A$，都有 $x \leqslant_A y \Rightarrow f(x) \leqslant_B f(y)$，则称 $f$ 是单调递增函数
  - 如果对于任意的 $x, y \in A$，都有 $x <_A y \Rightarrow f(x) <_B f(y)$，则称 $f$ 是严格单调递增函数

  类似可定义单调递减函数和严格单调递减函数。
- 泛函：称 $f: A \to C^B$ 称为一个泛函。
  比如：令 $F: \mathbb{R} \to \mathbb{R}^{\mathbb{R}}, F(a) = (f_a(x) = x + a)$，$F$ 也可以写成：$F: a \to [x \to a]$:
  - $F(1) = f_1(x) = x + 1$
  - $F(2)(3) = f_2(3) = 3 + 2 = 5$



## 单射、满射、双射



在目前函数的定义上，我们要求了 $\mathrm{dom}(f) = A$，即每一个 $A$ 中的元素都有唯一的一个函数值。下面我们再定义基于此的一些函数的性质，

**定义 6** [单射 (Injective/One-to-one)].
令 $f: A \to B$，如果对于任意的 $x, y \in A$，都有 $f(x) = f(y) \Rightarrow x = y$，则称 $f$ 是单射。

**定义 7** [满射 (Surjective/Onto)].
令 $f: A \to B$，如果对于任意的 $y \in B$，都存在 $x \in A$ 使得 $f(x) = y$，则称 $f$ 是满射。

**定义 8** [双射 (Bijective/One-to-one correspondence)].
令 $f: A \to B$，如果 $f$ 是单射且满射，则称 $f$ 是双射。双射也被称为一一映射。



## 一些例子 (I)



**例 9.**
请判断，下列函数是否为单射、满射、双射。

1. $f_1: \mathbb{R} \to \mathbb{R}$, $f_1(x) = x^2$.
2. $f_2: \mathbb{Z}^+ \to \mathbb{R}$, $f_2(x) = \ln x$.
3. $f_3: \mathbb{R} \to \mathbb{Z}$, $f_3(x) = \lceil x \rceil$.
4. $f_4: \mathbb{R} \to \mathbb{R}$, $f_4(x) = 2x + 1$.

**解 10.**
1. $f_1$ 不是单射，也不是满射。
2. $f_2$ 是单射，但是不是满射。
3. $f_3$ 是满射，但是不是单射。
4. $f_4$ 是双射。



## 一些例子 (II)



**例 11.**
请根据下列集合 $A$ 和 $B$ 给出一个函数 $f: A \to B$，使得 $f$ 是双射。

1. $A = \{1,2,3\}$, $B = \{a,b,c\}$.
2. $A = \mathscr{P}(\{1,2,3\})$, $B = \{0,1\}^{\{1,2,3\}}$
3. $A = \mathbb{Z}$, $B = \mathbb{N}$.
4. $A = (-\frac{\pi}{2}, \frac{\pi}{2})$, $B = \mathbb{R}$

**解 12.**
1. $f = \{(1,a),(2,b),(3,c)\}$.
2. $f = \{(A_i, f_i)\}$.
3. $f = \begin{cases} 2x+1, & x \geqslant 0 \\ -2x, & x < 0 \end{cases}$.
4. $f = \tan x$.

# 函数的复合和逆运算



函数是一种特殊的关系，因此我们也可以在其上面进行复合与逆运算。先来考虑复合运算。

**定理 13** **[函数的复合].**

给定两个函数 $f: A \to B$ 和 $g: B \to C$，则:

1. 其复合 $f \circ g$ 也是函数。
2. $f \circ g(x) = g(f(x))$.

**额外说明**

可以看到，由于我们关系的定义用的是右复合，所以我们会有:

$$f \circ g(x) = g(f(x))$$

有的书上会用左复合，则函数复合的形式会转换为: $f \circ g(x) = f(g(x))$.



# 函数的复合



**证明.**

1. 我们先证明 $f \circ g$ 是个函数。
   - $\forall x \in A$，存在 $y \in B$ s.t. $f(x) = y$. 由于 $g$ 是函数，从而存在 $z \in C$ s.t. $g(y) = z$，因此 $(x, z) \in f \circ g$，即 $\mathrm{dom}(f \circ g) = A$.
   - 假设存在 $x \in A$ s.t. $(x, y_1), (x, y_2) \in f \circ g$，则存在 $z_1$，$z_2 \in B$ s.t. $(x, z_1), (x, z_2) \in f, (z_1, y_1), (z_2, y_2) \in g$，由函数的定义 $z_1 = z_2$，从而 $y_1 = y_2$，即 $f \circ g$ 是函数。
2. 对任意的 $x \in A$，我们有 $(x, f(x)) \in f, (f(x), g(f(x))) \in g$，从而 $(x, g(f(x))) \in f \circ g$，即 $f \circ g(x) = g(f(x))$.

□



# 函数的逆



**定理 14** **[函数的逆].**

给定函数 $f: A \to B$，则 $f^{-1}$ 也是函数当且仅当 $f$ 是双射。

**证明.**

- $(\Rightarrow)$ 假设 $f^{-1}$ 是函数。则对于任意的 $y \in B$，都存在 $x \in A$ s.t. $f^{-1}(y) = x$，即 $f(x) = y$，从而 $f$ 是满射。$f$ 是单射则是显然的，否则:

$$(x_1, y), (x_2), y \in f \Rightarrow (y, x_1), (y, x_2) \in f^{-1}$$

  从而 $f^{-1}$ 不是函数。因此 $f$ 是双射。
- $(\Leftarrow)$先证 $f^{-1}$ 的定义域是$B$。

$$\forall x \in B \exists y \in A \ f(y) = x \Rightarrow f(x) = y \Rightarrow x \in \mathrm{dom}(f^{-1}) \Rightarrow \mathrm{dom}(f^{-1}) = B$$

  再证 $f^{-1}$ 是函数。若 $(x, y_1), (x, y_2) \in f^{-1}$，则 $(y_1, x), (y_2, x) \in f$，从而 $y_1 = y_2$，即 $f^{-1}$ 是函数。

□



# 函数的复合和反函数-—些例子



**定义 15** **[反函数].**

对于一个双射 $f: A \to B$，我们称其逆 $f^{-1}$ 为反函数。

**例 16.**

令 $f(x) = x + 2$, $g(x) = x^2$ 都是 $\mathbb{R} \to \mathbb{R}$ 的函数，则我们有:

- $f$ 的反函数为 $f^{-1}(x) = x - 2$.
- $g$ 不是双射，因此不存在反函数。
- $f \circ g(x) = g(f(x)) = x^2 + 4x + 4$
- $g \circ f(x) = f(g(x)) = x^2 + 2$

## 函数复合和反函数的性质



**定理 17.**
给定函数 $f: A \to B$，$g: B \to C$，则：

1. 若 $f$ 和 $g$ 都是单射，则 $f \circ g$ 也是单射。
2. 若 $f$ 和 $g$ 都是满射，则 $f \circ g$ 也是满射。
3. 若 $f$ 和 $g$ 都是双射，则 $f \circ g$ 也是双射。
4. $f = f \circ I_B = I_A \circ f$
5. 若 $f$ 是双射，则有 $f \circ f^{-1} = I_A$，$f^{-1} \circ f = I_B$.



## 函数复合和反函数的性质



**证明.**

1. 假设存在 $x_1, x_2 \in A$ s.t. $f \circ g(x_1) = f \circ g(x_2)$，则 $g(f(x_1)) = g(f(x_2))$，由于 $g$ 是单射，从而 $f(x_1) = f(x_2)$，由于 $f$ 是单射，从而 $x_1 = x_2$，即 $f \circ g$ 是单射。
2. 对 $\forall x \in C$，存在 $y \in B$ s.t. $g(y) = x$，由于 $f$ 是满射，从而存在 $z \in A$ s.t. $f(z) = y$，从而 $f \circ g(z) = x$，即 $f \circ g$ 是满射。
3. 由上述性质立马可得。
4. 只证 $f = f \circ I_B$.
$$(x,y) \in f \Leftrightarrow (x,y) \in f \wedge (y,y) \in I_B \Leftrightarrow (x,y) \in f \circ I_B$$
5. 只证 $f \circ f^{-1} = I_A$.
$$(x,y) \in f \circ f^{-1} \Leftrightarrow \exists z (x,z) \in f \wedge (z,y) \in f^{-1} \Leftrightarrow (z,x),(z,y) \in f^{-1} \Leftrightarrow x = y \Leftrightarrow (x,y) \in I_A$$

$\square$



## 集合基数

## 无限集合的衡量



判断有限集合之间的大小我们可以用元素个数来衡量，但是对于无限集合，我们该如何衡量其大小呢？

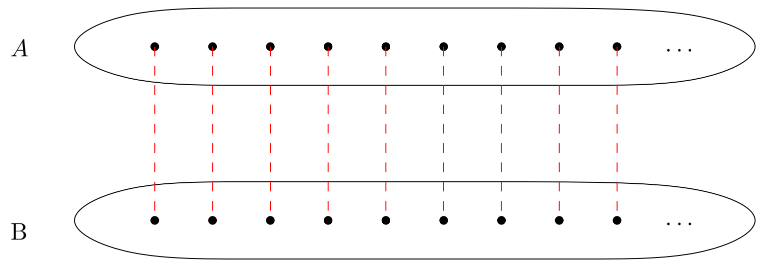
- $\mathbb{N}$，$\mathbb{Q}$，$\mathbb{R}$ 哪个更大？

我们利用双射函数的概念来对无限集合进行比较。

## 集合等势

**定义 18** **[集合等势].**

令 $A, B$ 是两个集合，如果存在一个双射 $f: A \to B$，则称 $A$ 与 $B$ 等势，记作 $A \approx B$，若 $A$ 和 $B$ 不等势，则记作 $A \not\approx B$.



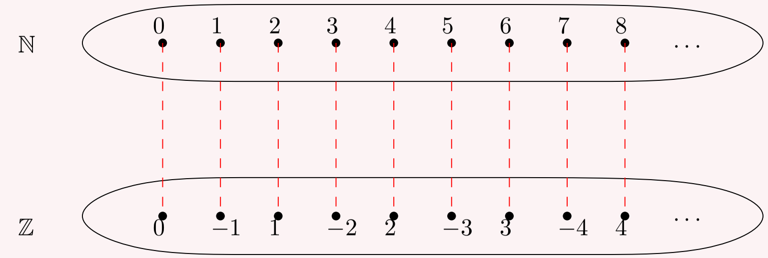

显然等势关系满足自反性、对称性、传递性，从而其是一个等价关系。



## 等势集合的例子 (I)

**例 19.**

1. $\mathbb{N} \approx \mathbb{Z}$.



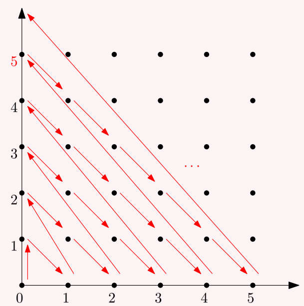

- $f: \mathbb{N} \to \mathbb{Z}, \quad f(n) = \begin{cases} \frac{n}{2}, & n\text{为偶数} \\ -\frac{n+1}{2}, & n\text{为奇数} \end{cases}$



## 等势集合的例子 (II)

**例 20.**

2. $\mathbb{N} \approx \mathbb{N} \times \mathbb{N}$.




- $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

  $f((m.n)) = \frac{(m+n+1)(m+n)}{2} + m$

**推论 21.**

$\mathbb{N} \approx \mathbb{Q}$.



## 等势集合的例子 (III)

**例 22.**

3. $(0,1) = [0,1] = [a,b] = \mathbb{R}$，这里 $a, b \in R$

- $[0,1] \approx [a,b]$ 是简单的，考虑 $f: [0,1] \to [a,b]$，$f(x) = a + (b-a)x$ 即可。
- $(0,1) \approx \mathbb{R}$ 也是简单的，考察 $\tan$ 函数，考虑 $f: (0,1) \to \mathbb{R}, f(x) = \tan(\frac{2x-1}{2}\pi)$ 即可。
- 最后我们来说明 $[0,1] \approx (0,1)$. 考虑

$$f: [0,1] \to (0,1),\ f(x) = \begin{cases} \frac{1}{2}, & x = 0 \\ \frac{1}{n+1}, & x = \frac{1}{n},\ n \in \mathbb{N} \\ x, & \text{otherwise} \end{cases}$$

$f$ 是个双射函数。

## 集合等势的性质



我们现在来关注一下幂集的性质。

**定理 23.**
对于任意的集合 $A$，都有 $\{0,1\}^A \approx \mathscr{P}(A)$.

上述定理说明，$A$ 的子集组成的集合与 $A$ 到 $\{0,1\}$ 的函数集合等势.

**证明.** 构造 $\mathscr{P}(A) \to \{0,1\}^A$ 的函数如下：$f(A') = \chi_{A'}$，这里 $\chi_{A'}$ 是 $A'$ 的特征函数。

- $f$ 是单射。若 $A' \neq A''$，则存在 $x \in A'$ s.t. $x \notin A''$，从而 $f(A')(x) = 1$，$f(A'')(x) = 0$.
- $f$ 是满射。对于任意的 $g \in \{0,1\}^A$，令 $B = \{x \in A \mid g(x) = 1\}$，则 $f(B) = \chi_B = g$.

□



## 康托定理



**定理 24** [Cantor,1873].
$\mathbb{N} \not\approx \mathbb{R}$

**证明.** 假设存在 $\mathbb{N}$ 到 $\mathbb{R}$ 的双射 $f$，即 $f$ 可以表示如下：

$$\begin{aligned} f(0) &= b_1.a_{11}a_{12}a_{13}\ldots \\ f(1) &= b_2.a_{21}a_{22}a_{32}\ldots \\ f(2) &= b_3.a_{31}a_{32}a_{33}\ldots \\ &\ldots \end{aligned}$$

这里假设每一个实数都是无限循环的小数，则我们考虑下面的实数 $x = 0.c_1c_2c_3\cdots$ 满足：

$$c_i \neq a_{ii}$$

由定义，不存在任何 $n \in \mathbb{N}$ 使得 $f(n) = x$。这与 $f$ 是双射矛盾，因此 $\mathbb{N} \not\approx \mathbb{R}$. □ 通过相似的证明可以得出 $\mathscr{P}(A) \not\approx A$. 这种方法被称作对角线方法。



## 集合的比较



由康托定理，我们可以得出 $\mathbb{N}$ 和 $\mathbb{R}$ 的大小不同，但直观上我们可以看出 $\mathbb{R}$ 比 $\mathbb{N}$ 要大，那么我们如何衡量集合的大小呢?

**定义 25.**
令 $A, B$ 是两个集合，

- 如果存在 $A$ 到 $B$ 的单射函数，则称 $B$ 优势于 $A$，记作 $A \preceq B$，若 $B$ 不优势于 $A$，则记作 $A \npreceq B$.
- 如果存在 $A$ 到 $B$ 的单射函数并且 $A \not\approx B$，则称 $B$ 真优势于 $A$，记作 $A \prec B$，若 $B$ 不真优势于 $A$，则记作 $A \nprec B$

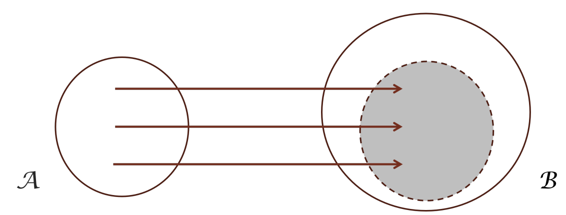


## 集合的比较例子



**例 26.**
1. $\mathbb{N} \preceq \mathbb{R}$, $\mathbb{N} \prec \mathbb{R}$.
2. $A \preceq A$, $A \nprec A$.
3. 如果 $A$ 是 $B$ 的子集，则 $A \preceq B$.

**引理 27.**
集合 $B$ 优势于 $A$ 当且仅当 $A$ 和某个 $B$ 的子集 $B'$ 等势.



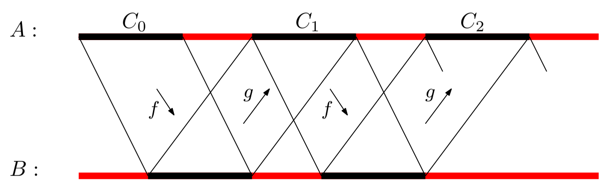
## Schröder-Bernstein 定理

**定理 28** **[Schröder-Bernstein 定理].**
如果 $A \preceq B$ 且 $B \preceq A$，则 $A \approx B$.

**证明.** 假设存在 $A$ 到 $B$ 的单射 $f$，$B$ 到 $A$ 的单射 $g$，递归定义集合 $C_i$:

$$C_0 = A - \mathrm{ran}(g),\ C_{i+1} = g(f(C_i))$$

考察如下函数：$h(x) = \begin{cases} f(x) & x \in C_i \\ g^{-1}(x) & \text{otherwise} \end{cases}$，则 $h(x)$ 是一个 $A$ 到 $B$ 的双射。




□



## 集合的基数 (I)

我们将自然数 $n \in \mathbb{N}$ 看成如下的集合 $\{0, 1, 2, \ldots, n-1\}$，结合之前的对有限集和双射的讨论，我们可以统一来定义集合的基数。

**定义 29** **[集合基数].**
对于集合 $A, B$，其基数分别用 $\mathrm{card}(A), \mathrm{card}(B)$ 表示，满足:

$$\mathrm{card}(A) = \mathrm{card}(B) \Leftrightarrow A \approx B$$

特别的，

- 若集合 $A$ 与某个自然数 $n$ 等势，则 $A$ 的基数记作 $\mathrm{card}(A) = n$.
- 自然数集合 $\mathbb{N}$ 的基数记作 $\aleph_0$.
- 实数集合 $\mathbb{R}$ 的基数记作 $\aleph 1$.



## 集合的基数 (II)

我们现在来定义基数的大小。

**定义 30.**
令 $A, B$ 为集合，则我们有:

1. $\mathrm{card}(A) \leqslant \mathrm{card}(B) \Leftrightarrow A \preceq B$.
2. $\mathrm{card}(A) < \mathrm{card}(B) \Leftrightarrow \mathrm{card}(A) \leqslant \mathrm{card}(B) \wedge \mathrm{card}(A) \neq \mathrm{card}(B)$.

- 我们将基数为某个自然数的集合称作有限集合，这类基数也称作有穷基数。
- 无穷集合的基数如 $\aleph_0, \aleph_1, \ldots$ 称作无穷基数。

是否存在比 $\aleph$ 更大的基数？存在，比如 $\mathscr{P}(\mathbb{R})$ 的基数。



## 可数集与不可数集

我们来关注一类特殊的无穷集-可数集。

**定义 31.**
令 $A$ 为集合，若 $\mathrm{card}(A) \leqslant \aleph_0$，则称 $A$ 是可数集或者可列的集合。

**可数集的直观理解**
直观上来说，可数集如同自然数集一般，我们可以挨个将其列举出来，即有一种办法将其全部枚举。

**定义 32** **[等价定义].**
$A$ 是可数集当且仅当 $A \approx \mathbb{N}$ 或者 $A$ 是有限集.

## 可数集举例

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ 是可数的。
- $\mathbb{R}$ 是不可数的。
- 若 $A, B$ 是可数的，则 $A \cup B$，$A \times B$ 是可数的。。
- 可数个可数集的并依旧是可数的。
- 对于任意的无穷集合 $A$，$A$ 的幂集 $\mathscr{P}(A)$ 是不可数的。

**问题 33** **[连续统假设 (Continuum Hypothesis,CH)].**

不存在一个集合 $A$ 满足 $\aleph_0 < \mathrm{card}(A) < 2^{\aleph_0}(\aleph_1)$.

**关于连续统假设**

- 这是 Hilbert 提出的 23 个问题中的第一个问题。
- 目前已经被证明，在现有的公理化系统下，既不能证明是对的，也不能证明是错的。($ZFC \nvdash CH$，$ZFC \nvdash \neg CH$)



## 可计算性理论简介

## 计算机能写出什么样的程序？

假设给出下面这些问题，我们能否写出一个程序来解决这些问题？

- 输入两个整数，求这两个整数的和。
- 输入三个实数，判断第三个数是不是前两个数的和。
- 输入一个一阶逻辑公式，求其前束范式。
- 输入两个一阶逻辑公式，判断第二个逻辑公式是否是第一个逻辑公式的前束范式。
- 输入一个程序，判断其是否会陷入死循环。

**计算机的能力？**

上述问题其实询问的是计算机的能力，其实际上蕴含了两个方面的内容：

1. 这个问题可以被计算机解决吗？
2. 如果目前不能解决，如果有了更新的计算机，比如量子计算机，能否解决？



## 形式化的考虑计算能力

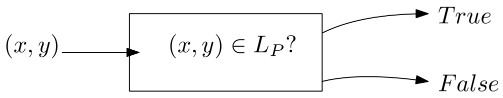
实际上计算机的程序的行为可以如下所示：

$$Input : x \longrightarrow \boxed{\text{Program P}} \longrightarrow Output : y$$

这样一个程序实际上解决的是一个集合的元素归属问题，即：

- 令 $L_P = \{(x, y) | y$ 是 $x$ 输入程序 $P$ 产生的输出$\}$，程序实际上解决的便是 $(x, y) \in L_P$？

## 计算能力 → 语言识别能力




- 我们可以进一步把 $(x,y)$ 看成一个串 $w$，假设其字母表为 $\mathcal{A}$。
- 令 $L_P$ 是 $\mathcal{A}$ 上的一个串的集合，$L_P$ 称为一个语言 (language)。
- 一个问题实际上便转化成了问：$w \in L_P$，即这种语言是否能被识别 (recongnize)?

~~计算机能解决什么问题?~~

↓

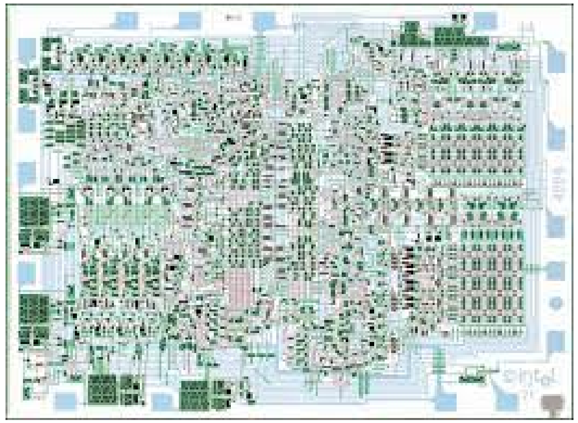
计算机能识别什么语言?



## 计算机的抽象-计算模型 (I)

我们再来考虑一下计算机本身。

图: Intel 4004-第一款商用芯片





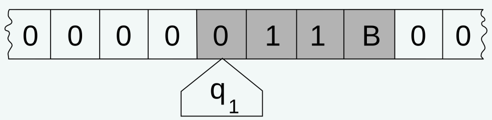
## 计算机的抽象-计算模型 (II)

实际中的计算机是非常复杂的，因此我们会在一些抽象的计算模型上讨论。

- 自动机 (Automata)
- 图灵机 (Turing Machine)
- λ-演算 (λ-Calculus)
- ...

**图灵机**

图灵机是英国数学家艾伦·图灵于 1936 年提出的一种将人的计算行为抽象化的数学逻辑机，其更抽象的意义为一种计算模型。




我们忽略图灵机的具体细节，只要认识到我们目前能在计算机上写的任何程序都可以用图灵机实现即可。



## 可计算函数

我们现在来可以定义可计算的概念了。

**定义 34** **[图灵可识别语言 (Turing Recognizable)].**
对于一个语言 L，如果存在一台图灵机能接受该语言，即对于任意的 $w \in L$，图灵机能输出 1(True)，则称 L 是图灵可识别的。

**定义 35** **[图灵可判定语言 (Turing Decidable)].**
对于一个语言 L，如果存在一台图灵机能判定该语言，即对于任意的 $w \in L$，图灵机能输出 1(True)，并且对于任何 $w \notin L$，图灵机能停机并输出 0(False)，则称 L 是图灵可判定的。

我们将由图灵机可判定的函数称作可计算函数 (computable function)。

## 一些例子

为了方便例子叙述，假设字母表是 $\{0,1,\#\}$

- $L=\{0^n|n\geqslant 0\}$ 是图灵可识别的，也是图灵可判定的。
- $L=\{x|x$ 是回文串$\}$ 是图灵可识别的，也是图灵可判定的。
- $L=\{x\#y\#z|z=x+y\}$ 是图灵可识别的，也是图灵可判定的。

回到我们最初的问题，存不存在图灵不可判定的、甚至是图灵不可识别的语言？

Yes!



## 停机问题

**定理 36.**
令 $\mathrm{Halt}_{TM}=\{(M,\omega)\mid$ 图灵机 $M$ 在输入 $\omega$ 上能停机$\}$。$\mathrm{Halt}_{TM}$ 是不可判定的。

这就是停机问题 (Halting Problem) 的叙述。

**证明.** 假设存在一个图灵机 $H$，使得 $H$ 能判定 $\mathrm{Halt}_{TM}$，即我们有:

$$H(M,\omega)=\begin{cases}1, & \text{如果 } M \text{ 能在输入 } \omega \text{ 上停机}\\ 0, & \text{如果 } M \text{ 能在输入 } \omega \text{ 上不停机}\end{cases}$$

我们来构造一台新的图灵机 $D$.



## 停机问题的证明 (II)

**证明. 续.** $D$ 的构造如下，假设对其输入一个图灵机 $\langle M\rangle$(我们用 $\langle M\rangle$ 来表示图灵机 $M$ 的一个串表示):

1. 运行 $H(M,\langle M\rangle)$，即调用 $H$ 运行图灵机 $M$ 在输入为它自己 $\langle M\rangle$ 时是否会停机。
2. 输出 $H(M,\langle M\rangle)$ 运行相反的结果，即如果 $H(M,\langle M\rangle)=1$，则运行一个死循环；反之，输出 $1$。

即:

$$D(\langle M\rangle)=\begin{cases}1, & \text{如果 } M \text{ 在输入 } \langle M\rangle \text{ 上不停机}\\ \text{死循环}, & \text{如果 } M \text{ 在输入 } \langle M\rangle \text{ 上停机}\end{cases}$$

但是我们有:

$$D(\langle D\rangle)=\begin{cases}1, & \text{如果 } D \text{ 在输入 } \langle D\rangle \text{ 上不停机}\\ \text{死循环}, & \text{如果 } D \text{ 在输入 } \langle D\rangle \text{ 上停机}\end{cases}$$

□



## 停机问题的证明-就是对角线方法!

我们再用图的方式看一下这个证明。为了方便叙述，令 $\infty$ 表示陷入死循环。

| | $\langle M_1\rangle$ | $\langle M_2\rangle$ | $\langle M_3\rangle$ | $\langle M_4\rangle$ | $\cdots$ | $\langle D\rangle$ |
|---|---|---|---|---|---|---|
| $M_1$ | 1 | $\infty$ | 1 | $\infty$ | | 1 |
| $M_2$ | $\infty$ | 1 | 1 | 1 | | $\infty$ |
| $M_3$ | 1 | 1 | $\infty$ | 1 | | 1 |
| $M_4$ | $\infty$ | 1 | 1 | $\infty$ | | 1 |
| $\vdots$ | | | | $\vdots$ | | |
| $D$ | $\infty$ | $\infty$ | 1 | 1 | | ? |
| $\vdots$ | | | | $\vdots$ | | |

- 上述图中的第 $i$ 行第 $j$ 列的元素表示 $M_i$ 在输入 $\langle M_j\rangle$ 是否停机，即 $H(M_i,\langle M_j\rangle)$ 的输出。
- 如果 $D$ 在里面，“?”这个位置到底应该是 $1$ 还是 $\infty$ 呢?

## 其他的不可判定问题



事实上，不可判定的问题远远多于可判定的问题，比如：

- $A_{TM} = \{\langle M, \omega\rangle \mid$ 图灵机 $M$ 能接受 $\omega\}$。
- $E_{TM} = \{\langle M\rangle \mid$ 图灵机 $M$ 能接受空串 $\epsilon\}$。
- $L = \{M \mid M$ 对于长度为 $n$ 的输入可以在 $n^2 + 100n + 92$ 的时间内输出结果$\}$.
- (希尔伯特第 10 问题) 丢番图方程是否有整数解？
- ...

不过上述问题虽然都是图灵不可判定的，但其实他们都是图灵可识别的，为什么？可以慢慢枚举出答案!

有没有图灵不可识别的语言呢？Yes!

**定理 37.**
$\overline{A_{TM}}$ 是图灵不可识别的。



## 丘奇-图灵论题 (Church – Turing thesis)



截至到目前，我们对于可计算性的讨论都是基于图灵机这一模型的，那如果换一个模型，计算能力会不会更强？

- 比如，量子计算机会不会比图灵机的计算能力更强？这里的更强的指的是能识别、判定更多的语言。

No!

**丘奇-图灵论题 (Church – Turing thesis)**
可计算函数就是图灵机可计算函数，或者说，任何物理可实现的计算就是图灵机可计算。

丘奇-图灵论题告诉我们，可计算这一概念实际上是独立于计算模型的，也就是说我们没有必要区分比如图灵可计算、量子计算机可计算等等，只需要一个可计算的概念就可以了。



## 总结



**本章总结**

- 函数的基本概念。
  - 函数的定义。
  - 单射、双射、满射。
  - 函数的复合和反函数。
- 集合的基数
  - 等势的概念。
  - 集合的比较。
  - 可数集与不可数集
- 可计算性理论简介
  - 计算能力与计算模型。
  - 图灵可识别性与图灵可判定性。
  - 不可判定问题。
  - 丘奇-图灵论题