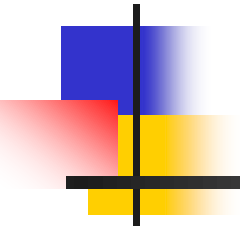


计算机科学导论

孙晓明

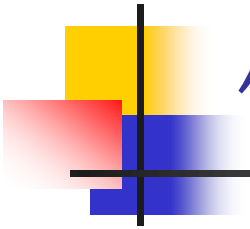
中国科学院计算技术研究所

2022-4-1

问题

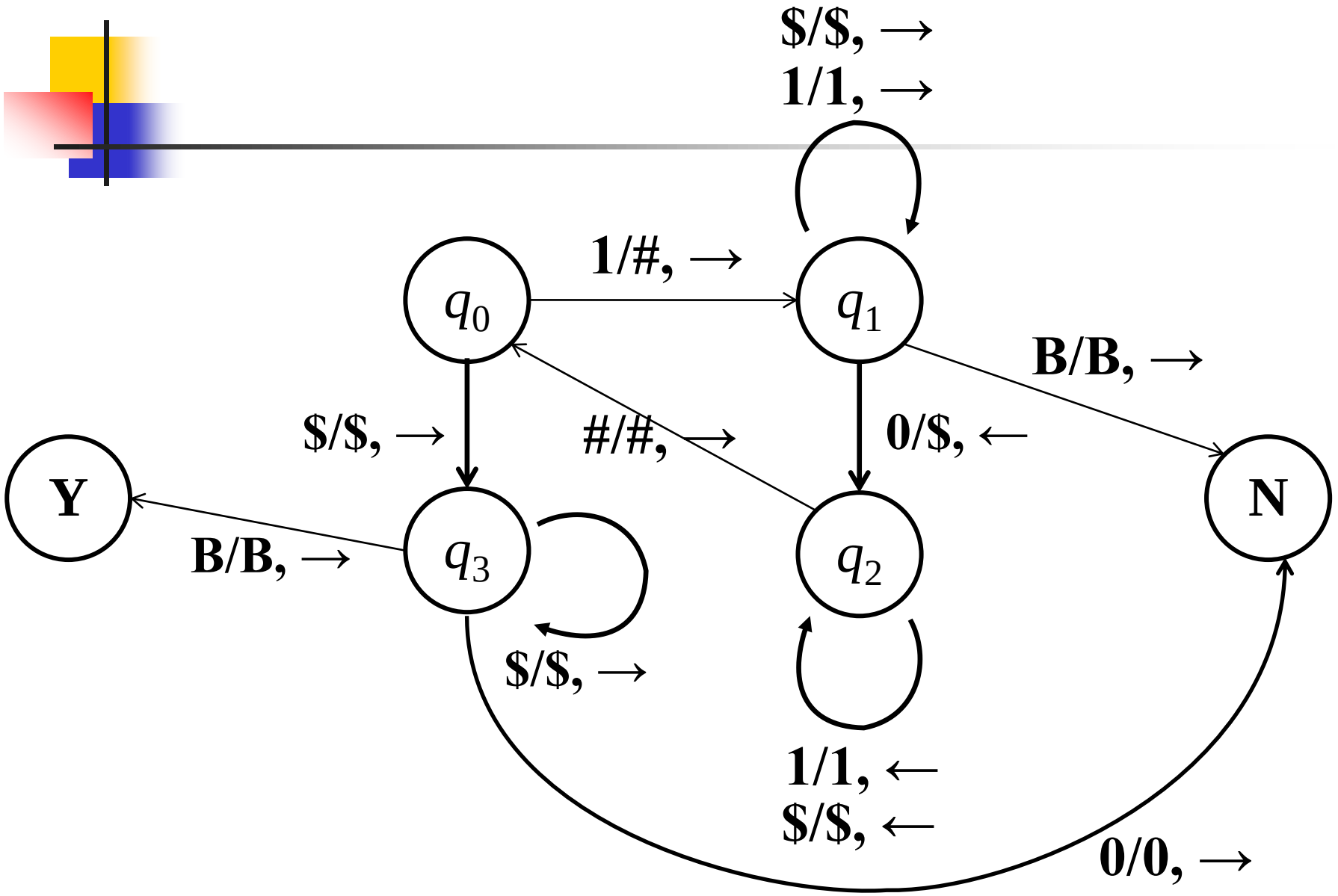
- 控制器只有一个状态、纸带上只有一个字符0的图灵机最多能运行多少步？

- 1) 2
- 2) 4
- 3) 16
- 4) $+\infty$



例4

- 输入：111…11000…00，判断1和0的个数是否相等？


$/$, →
1/1, →
1/#, →
q_0
q_1
B/B, →
$/$, →
#/#, →
0/$, ←
Y
N
B/B, →
q_3
q_2
$/$, →
1/1, ←
$/$, ←
0/0, →

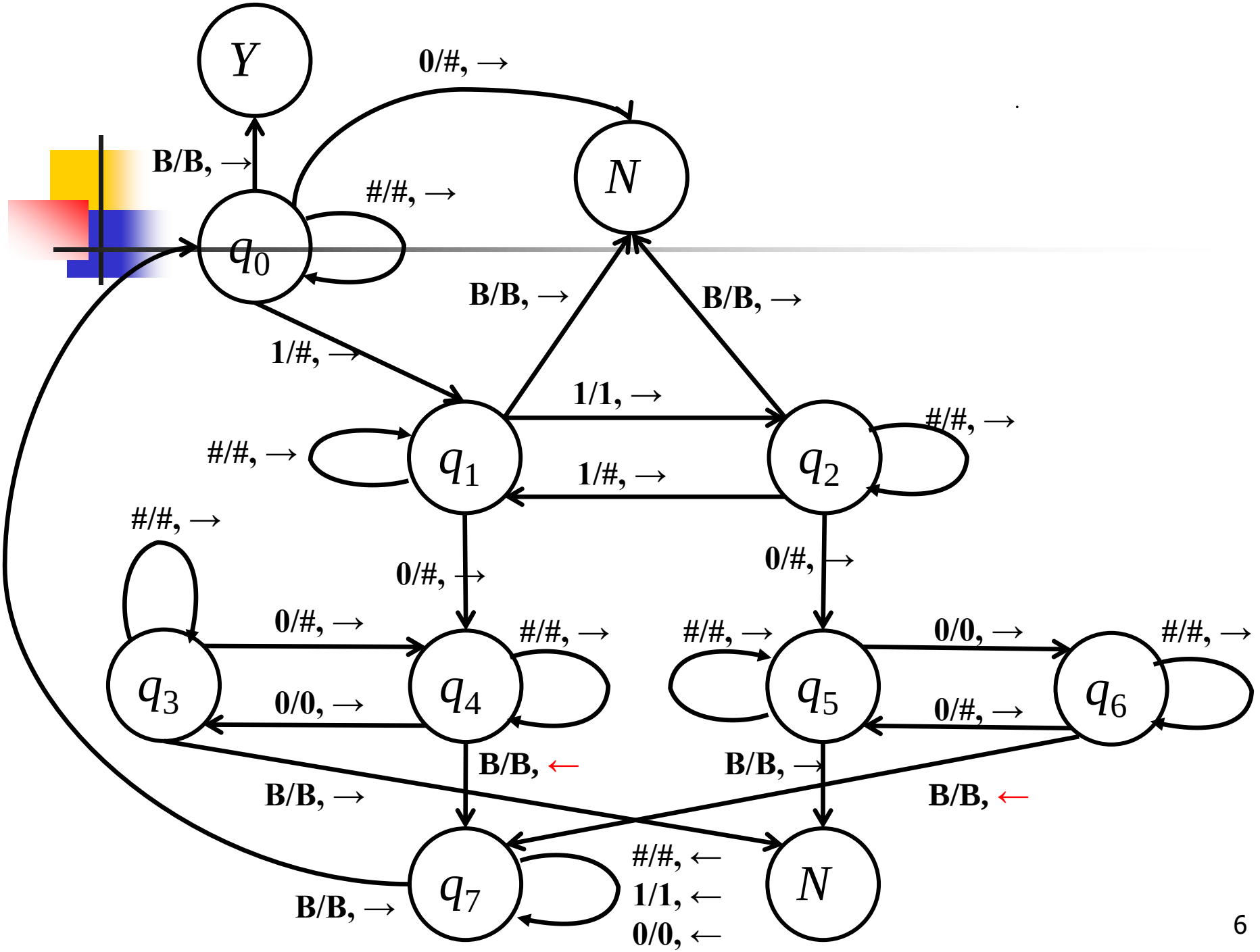
思考题

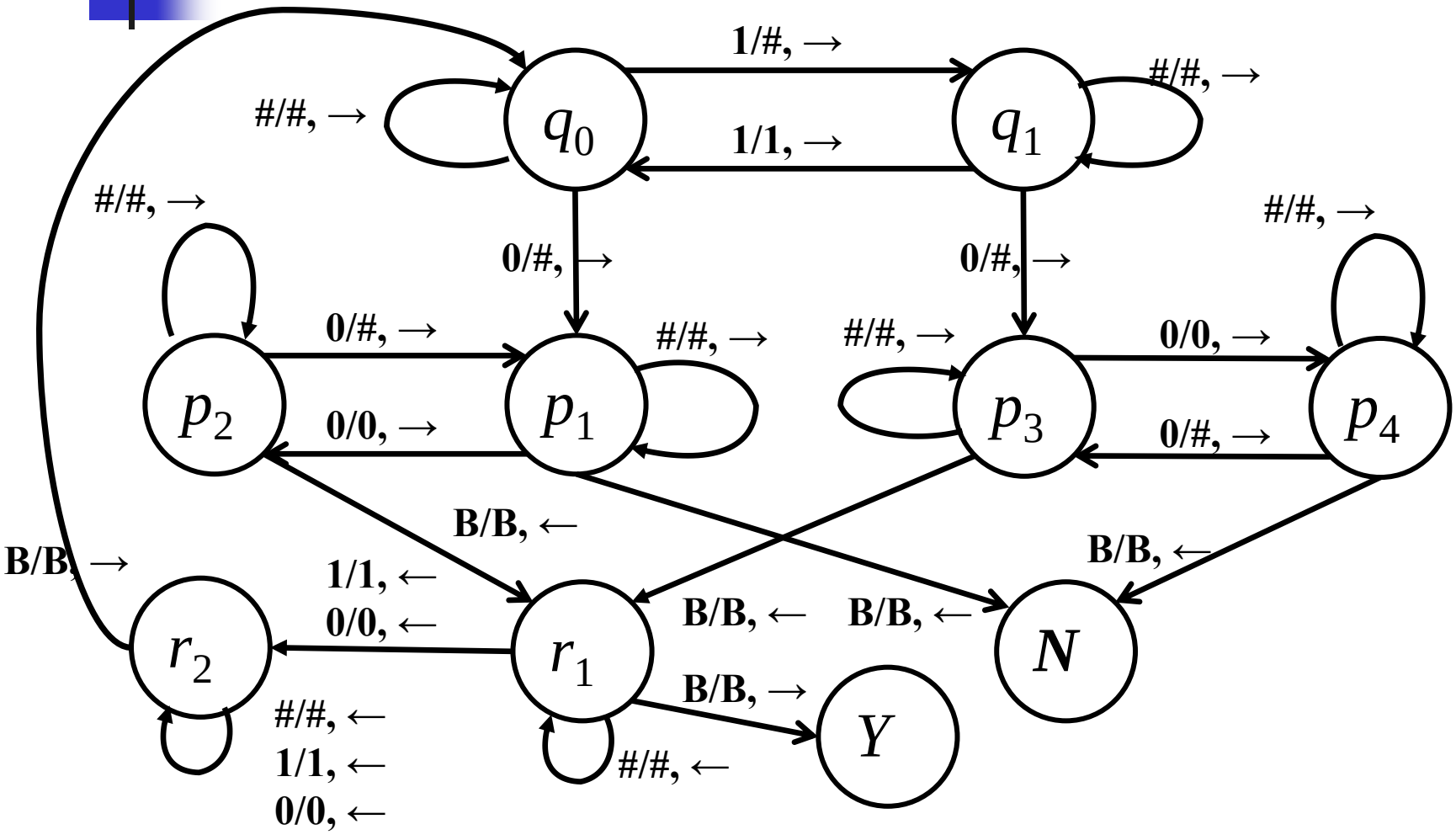
- 上面的图灵机判断 1^n0^n 需要花费~$2n^2$ 的时间，是否能够做的更快？

- Yes.
- Idea: 对于形如输入1^m0^n的输入，将m和n分别写成二进制数

  $m = m_s m_{s-1} \cdots m_1, n = n_t n_{t-1} \cdots n_1$

  然后逐位判定$m_i = n_i$，以及 $s = t$


Y
N
q_0
q_1
q_2
q_3
q_4
q_5
q_6
q_7
N
B/B, →
0/#, →
#/#, →
1/#, →
1/1, →
0/0, →
0/#, →
B/B, ←
#/#, ←
1/1, ←
0/0, ←


q_0
q_1
p_2
p_1
p_3
p_4
r_2
r_1
N
Y
1/#, →
#/#, →
1/1, →
#/#, →
#/#, →
0/#, →
0/#, →
#/#, →
0/#, →
#/#, →
0/0, →
0/0, →
0/#, →
B/B, ←
B/B, ←
B/B, →
1/1, ←
0/0, ←
B/B, ←
B/B, ←
B/B, →
#/#, ←
1/1, ←
0/0, ←
#/#, ←

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

In §§ 9, 10 I give some arguments with the intention of showing that the computable numbers include all numbers which could naturally be regarded as computable. In particular, I show that certain large classes of numbers are computable. They include, for instance, the real parts of all algebraic numbers, the real parts of the zeros of the Bessel functions, the numbers π, e, etc. The computable numbers do not, however, include all definable numbers, and an example is given of a definable number which is not computable.

Although the class of computable numbers is so great, and in many ways similar to the class of real numbers, it is nevertheless enumerable. In § 8 I examine certain arguments which would seem to prove the contrary. By the correct application of one of these arguments, conclusions are reached which are superficially similar to those of Gödel†. These results

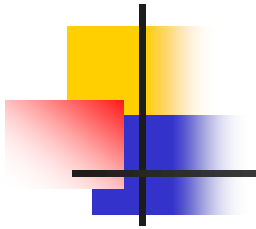
Alan Turing
1912-1954

- Turing Awards





2021 Turing Award: Jack Dongarra



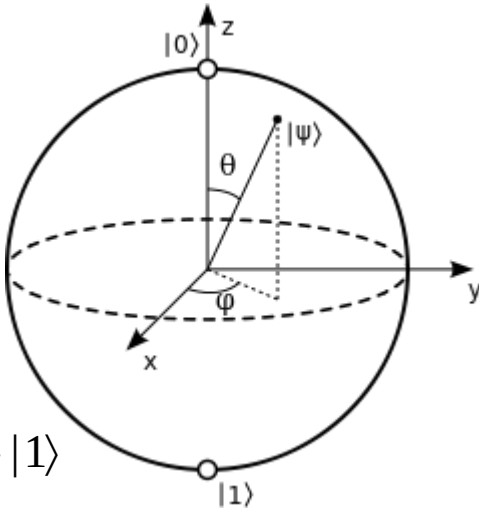
- Alonzo Church & Alan Turing:

  Church-Turing Hypothesis:

Any reasonable attempt to model mathematically computer algorithms and their performance is bound to end up with a model of computation and associated time cost that is equivalent to Turing machines within a polynomial.

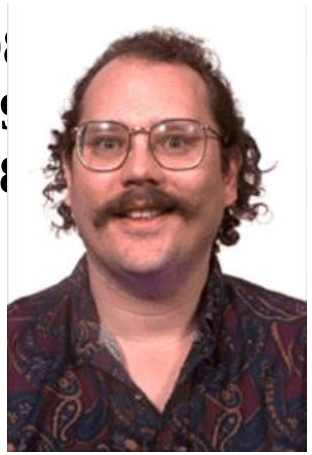
Alonzo Church
1903-1995

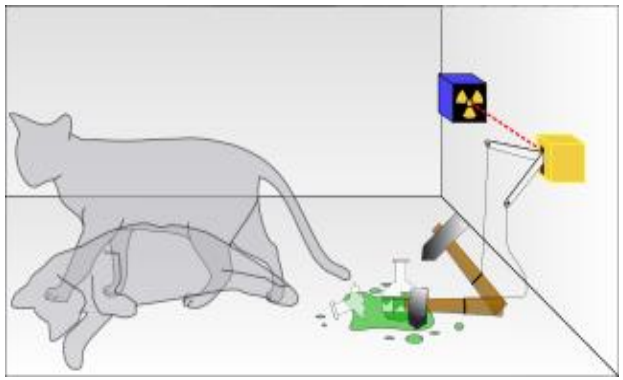
量子计算



$$\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$$

15226050279225336053561837813263
74297180681149613806886579084945801
22963258952897654000350692006139
=37975227936943673922808
62785456553663819 9×4009
08810306837352927614683
4061





Shor's factoring algorithm (1994): $O(\log^3 N)$ $O(2^{\log^{1/3} N})$

谓词逻辑

- 存在无穷多个素数。

Euclid of Alexandria

$$\forall n, \exists m, \forall p, q\,[(m > n) \wedge (p, q > 1 \rightarrow pq \neq m)]$$

谓词逻辑

- 存在无穷多个素数

$$\forall n, \exists m, \forall p, q[(m > n$$

- 对$n > 2$，丢潘图方程 $x^n + y^n = z^n$ 不存在非平凡解。

$$\forall a, b, c, n[(abc \neq 0) \wedge (n > 2) \rightarrow a^n + b^n \neq c^n]$$

- 存在无穷多对孪生素数。

$$\forall n, \exists m, \forall p, q\,[(m > n) \wedge (p, q > 1 \rightarrow (pq \neq m) \wedge (pq \neq m + 2)]$$

- 对任何一个正整数n，如果是奇数则乘3加1，如果是偶数则除2，重复此过程，最终将得到1。

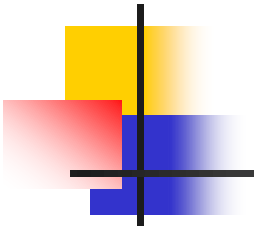
$$\forall n, \exists m, [f^{(m)}(n) = 1] \qquad f(n) = \begin{cases} 3n+1, & \text{if } n \equiv 1 (\text{mod } 2) \\ \dfrac{n}{2}, & \text{if } n \equiv 0 (\text{mod } 2) \end{cases}$$

3*n* + 1猜想

- 6 → 3 → 10 → 5 → 16 → 8 → 4 → 2 →1

- 15 → 46 → 23 → 70 → 35 → 106 → 53 →170 → 85 → 256 → 128 → 64 →32 → 16 → 8 → 4 → 2 → 1

- Solve it!!



- 四色定理：任何平面图都可以被四着色，使得任何两个相邻的顶点不同色。

$$\forall \text{平面图} G=(V,E), \exists c: V \to \{1,2,3,4\} \ \ \forall (u,v) \in E, [c(u) \neq c(v)]$$

- 图的3染色(3-coloring)：给定$G = (V, E)$

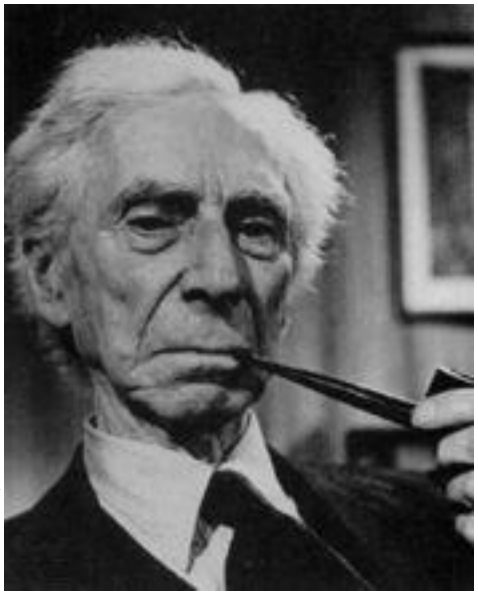
$$(\neg x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee \neg x_4 \vee \neg x_6) \wedge (x_2 \vee x_4 \vee \neg x_8) \wedge \ldots$$

- 可满足性问题(SAT)：给定CNF公式φ

$$\exists A: \{x_1, x_2, \ldots, x_n\} \to \{0,1\}, [\varphi(x_1, \ldots, x_n) = 1]$$

理发师悖论

- 在某个城市中有一位理发师我将为本城所有不给自己理，我也只给这些人理发。”
- 问题：这位理发师是否该给



Bertrand Russell

1872—1970

罗巴切夫斯基

- 公理系统：
  - 完备性，一致性（相容性）
- 欧几里德几何：
  - 公设1：任意一点到另外任意一点可以画直线
  - 公设2：一条有限线段可以继续延长
  - 公设3：以任意点为心及任意的距离可以画圆
  - 公设4：凡直角都彼此相等
  - 公设5：同平面内一条直线和另外两条直线相交，若在某一侧的两个内角和小于二直角的和，则这二直线经无限延长后在这一侧相交。

- David Hilbert (1900)
  - Tenth Problem: determine whether a given polynomial Diophantine equation with integer coefficients has an integer solution.

$$x^{17} + y^{17} = z^{17}$$
$$x^3 + y^3 = z^3 + w^3 + u^3$$
$$x^{2020} + y^{2021} = z^{2022}$$

David Hilbert
1862-1943

Hilbert 23 problems

- 1. 连续统假设
- 2. 算术公理的相容性
- 6. 物理科学的公理化
- 8. 黎曼猜想，歌德巴赫猜想，孪生素数猜想

Entscheidungsproblem

- 公理化系统的机械化判定问题（Hilbert 1928)
  - 可判定性：是否能够找到一种有效的方法（算法），判定一个数学命题是否为真?
  - 完备性
  - 一致性

Godel不完备性定理

- 定理一：任意一个包含一阶谓词逻辑与初等数论的形式系统，都不可能同时拥有完备性和一致性。即存在一个真命题，它在这个系统中不能被证明。
- 定理二：任意一个包含初等数论的系统S，当S无矛盾时，它的无矛盾性不可能在S内证明。

Kurt Godel

1906-1978

真和可以被证明是两件事情!!

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

In §§ 9, 10 I give some arguments with the intention of showing that the computable numbers include all numbers which could naturally be regarded as computable. In particular, I show that certain large classes of numbers are computable. They include, for instance, the real parts of all algebraic numbers, the real parts of the zeros of the Bessel functions, the numbers π, e, etc. The computable numbers do not, however, include all definable numbers, and an example is given of a definable number which is not computable.

Although the class of computable numbers is so great, and in many ways similar to the class of real numbers, it is nevertheless enumerable. In § 8 I examine certain arguments which would seem to prove the contrary. By the correct application of one of these arguments, conclusions are reached which are superficially similar to those of Gödel†. These results

Alan Turing
1936

可计算性

- 图灵机模型的计算能力
  - 有没有图灵机计算不了的问题？
  - Yes.

停机问题（Halting problem）：给定一台图灵机 M 和一个输入字符串 x，判定 M 在 x 这个输入上是否能够停机？（有限步终止）

没有图灵机能解决停机问题！

停机问题

- 假设有一台图灵机 M_H 能判定停机问题，即
  - $M_H(M,x)=1$，如果图灵机M在输入串x下能停机
  - $M_H(M,x)=0$，如果图灵机M在输入串x下不能停机

无论何种情况， M_H自身总是停机的！

停机问题

- 考察这样一台图灵机 $M_{\overline{H}}$(输入为x):

```
If (M_H(x, x)) {
    int i=1;
    while(true){
        i++;
    }
}
Return 1;
```

问题：在图灵机 $M_{\overline{H}}$上运行$M_{\overline{H}}$是否停机？

停机问题

111

	1	2	3	4	5	6	7	8	9	…
1	0	0	0	0	0	0	0	0	0	…
2	1	1	1	1	1	1	1	1	1	…
3	0	1	0	0	0	0	0	0	0	…
4	0	0	1	1	1	1	1	1	0	…
M_i 5	1	0	0	0	0	0	0	0	0	…
6	1	1	1	1	1	1	1	1	1	…
7	1	1	0	0	1	1	1	1	1	…
…	.	.	.	.	.	.	.	.	.	.

构造停机“真值表”：

第i号图灵机M_i

- 数字j的二进制编码串x^j
- 第i行第j列：M_i在x^j上会停机，则写1；否则写0

图灵机M_H就是在计算这张表

思考题

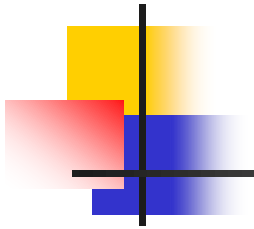
- Mr. S, Mr. P都具有足够的推理能力。约翰教授写了两个整数M和N (3≤M,N≤100)，并把M+N的值告诉了S先生，把M*N的值告诉了P先生。约翰教授问S先生和P先生：“你们能从已知的信息确定M和N的值吗？”

  S先生:” 我知道你不知道，我也不知道。”

  P先生:“现在我知道了。”

  S先生:“我也知道了。”

  请问，M和N是哪两个数？



谢谢！