

# 計算理論期末報告

Theory of Computation, NTHU

107021129 黃明瀧

此份報告的內容基於教科書 [1] 編寫，符號與定義多與教科書相同。部分證明細節取自上課教材 [2]。

## 1 $TM = NTM$

**定理 1** ( $TM = NTM$ )。給定任意的非確定型圖靈機<sup>1</sup> $N$ ，存在確定型圖靈機<sup>2</sup> $D$  使得  $L(N) = L(D)$ 。

*Proof.* 令  $N$  為一非確定型圖靈機。已知多帶圖靈機<sup>3</sup>與確定型圖靈機具有相同的計算能力，故若我們可以建構出多帶圖靈機  $D$  使得  $L(N) = L(D)$ ，則定理得證。以下我們以一多帶圖靈機  $D$  來模擬  $N$  的運算。

令  $D$  為一包含三條紙帶的多帶圖靈機，其中

- 紙帶 1 記錄原始輸入字串  $\omega$ 。
- 紙帶 2 記錄模擬的過程；類似於記憶體。

舉例來說， $0\#01$  代表目前紙帶上的字串為  $001$ ，且讀寫頭位於第二個字符的位置。

- 紙帶 3 記錄在計算樹<sup>4</sup>應選擇的分支。

舉例來說， $231$  代表應依序選擇根節點的第二個子節點、該子節點的第三個子節點、該子節點的第一個子節點來做運算。

紙帶 3 的字符集合  $\Gamma_b$  大小由  $N$  的計算樹的分歧度<sup>5</sup> $b$  所決定。 $b$  可以由  $N$  的狀態集及字符集推得。

$$b = |Q \times \Gamma \times \{L, R\}|$$

以下給出  $D$  的演算法文字敘述。對於輸入字串  $\omega$ ，

1. 將  $\omega$  寫至紙帶 1。初始化紙帶 2 及 3 為空。
2. 複製紙帶 1 的內容至紙帶 2，作為模擬用的輸入字串。
3. 依照紙帶 3 記錄的內容，在紙帶 2 上模擬  $N$  的運算。在模擬每一步驟之前，確認以下條件。

<sup>1</sup>非確定型圖靈機 = Nondeterministic Turing machine

<sup>2</sup>確定型圖靈機 = Deterministic Turing machine

<sup>3</sup>多帶圖靈機 = Multitape Turing machine

<sup>4</sup>計算樹 = Computation tree

<sup>5</sup>分歧度 = Degree

- a. 根據  $N$  之轉移函數  $\delta$ ，若此步驟為非法，則跳至步驟 4。
- b. 若紙帶 3 上已無任何字符，則跳至步驟 4。
- c. 根據  $N$  之拒絕狀態  $q_{\text{reject}}$ ，若目前模擬的狀態為拒絕狀態，則拒絕。
- d. 根據  $N$  之接受狀態  $q_{\text{accept}}$ ，若目前模擬的狀態為接受狀態，則接受。

4. 依照字典序，將紙帶 3 上的字串改為下一個字串。跳至步驟 2。

上述多帶圖靈機  $D$  會依序模擬  $N$  執行 0 步  $\rightarrow$  執行 1 步  $\rightarrow$  執行 2 步  $\dots$ ，以廣度優先的方式嘗試所有運算路徑，故  $D$  接受 (拒絕) 字串  $\omega$  若且唯若  $N$  接受 (拒絕) 字串  $\omega$ 。因此， $L(N) = L(D)$ 。□

## 2 Rice Theorem

**定理 2** (Rice's Theorem). 令  $P$  為一語言，使得下列兩條件成立，則  $P$  是不可判定<sup>6</sup>的。

1.  $P$  是非平凡<sup>7</sup>的；亦即存在圖靈機  $M$  使得  $\langle M \rangle \in P$ ，但不是所有的圖靈機的敘述都屬於  $P$ 。
2.  $P$  是語言的性質；亦即若  $L(M_1) = L(M_2)$ ，則  $\langle M_1 \rangle \in P \Leftrightarrow \langle M_2 \rangle \in P$ 。換句話說，一個圖靈機的敘述是否屬於  $P$ ，只與該圖靈機對應的語言有關。

*Proof.* 我們以反證法證明 Rice's Theorem。假設  $P$  是可判定的。令  $M_P$  為判定  $P$  的圖靈機。我們將使用  $M_P$  來建構出可判定  $A_{\text{TM}}$  的圖靈機。

令  $T_\emptyset$  為一拒絕所有輸入的圖靈機。 $L(T_\emptyset) = \emptyset$ 。不失一般性<sup>8</sup>，假設  $\langle T_\emptyset \rangle \notin P$ 。由條件 1，令  $T$  為圖靈機，使得  $\langle T \rangle \in P$ 。

利用  $P$  可以「分辨」出  $T_\emptyset$  與  $T$  之間差異的能力，對於輸入  $\langle M, \omega \rangle$ ，設計以下圖靈機  $S$ ，作為  $A_{\text{TM}}$  的判定器。

1. 利用  $M$  與  $\omega$  來建構圖靈機  $M_\omega$ ：

對於輸入  $x$ ，

- a. 以  $\omega$  作為輸入模擬  $M$  的執行。若  $M$  拒絕，則拒絕。
- b. 以  $x$  作為輸入模擬  $T$  的執行。若  $T$  接受，則接受。

2. 以  $M_P$  來判斷  $\langle M_\omega \rangle$  是否屬於  $P$ 。若  $\langle M_\omega \rangle \in P$ ，則接受。若  $\langle M_\omega \rangle \notin P$ ，則拒絕。

為什麼  $S$  可以判定  $A_{\text{TM}}$  呢？我們可以討論兩種情形，分析  $S$  的行為。

- 若  $M$  接受  $\omega$ ，則  $M_\omega$  會進入步驟 1b  $\Rightarrow L(M_\omega) = L(T) \Rightarrow \langle M_\omega \rangle \in P$
- 若  $M$  拒絕  $\omega$ ，則  $M_\omega$  會拒絕所有輸入字串  $x \Rightarrow L(M_\omega) = L(T_\emptyset) \Rightarrow \langle M_\omega \rangle \notin P$

<sup>6</sup>不可判定 = Undecidable

<sup>7</sup>非平凡 = Nontrivial

<sup>8</sup>若  $\langle T_\emptyset \rangle \in P$ ，則整個證明可以改以  $\bar{P}$  來進行，使得  $\langle T_\emptyset \rangle \notin P$ 。

我們可以看出  $\langle M_\omega \rangle \in P$  若且唯若  $M$  接受  $\omega$ ，因此  $S$  可以判定  $A_{TM}$ 。然而我們已知  $A_{TM}$  是一個不可判定的語言，所以此結論為矛盾。因此， $P$  不可判定。□

以下舉例說明如何使用 Rice's Theorem 證明  $INFINITE_{TM} = \{ \langle M \rangle \mid |L(M)| = \infty \}$  的不可判定性。

*Proof.* 要使用 Rice's Theorem，我們需要驗證  $INFINITE_{TM}$  是否符合定理的兩個前提。

1. 令  $T_{all}$  為接受所有輸入字串的圖靈機。因  $\langle T_{all} \rangle \in INFINITE_{TM}$  且  $\langle T_\emptyset \rangle \notin INFINITE_{TM}$ ，故  $INFINITE_{TM}$  是非平凡的。
2.  $INFINITE_{TM}$  的定義只與  $L(M)$  有關，故  $INFINITE_{TM}$  是語言的性質。

$INFINITE_{TM}$  符合 Rice's Theorem 的兩個前提，因此  $INFINITE_{TM}$  是不可判定的。□

### 3 Post Correspondence Problem

#### 3.1 PCP 問題簡述

PCP 問題建立在一個以骨牌進行的益智遊戲上。每張骨牌形如

$$\begin{bmatrix} t \\ \bar{b} \end{bmatrix} = \begin{bmatrix} a \\ ab \end{bmatrix}$$

分為上下兩個部分，分別載有一個字串。令  $P$  為一個骨牌的集合，例如

$$P = \left\{ \begin{bmatrix} b \\ ca \end{bmatrix}, \begin{bmatrix} a \\ ab \end{bmatrix}, \begin{bmatrix} ca \\ a \end{bmatrix}, \begin{bmatrix} abc \\ c \end{bmatrix} \right\}$$

。對於某些  $P$ ，我們可以找到一個（可重複的）骨牌排列方式，使得「骨牌上半的所有字符所組成的字串」與「骨牌下半的所有字符鎖組成的字串」相等。以前述  $P$  為例，

$$\begin{bmatrix} a \\ ab \end{bmatrix} \begin{bmatrix} b \\ ca \end{bmatrix} \begin{bmatrix} ca \\ a \end{bmatrix} \begin{bmatrix} a \\ ab \end{bmatrix} \begin{bmatrix} abc \\ c \end{bmatrix}$$

即為一個合法的**對應**<sup>9</sup>。判斷一個骨牌的集合  $P$  是否存在這樣的排列方式，即為波斯特對應問題。以形式語言的方式來說：

$$PCP = \{ \langle P \rangle \mid P \text{ 為一個存在對應的 Post Correspondence Problem 的實例} \}$$

<sup>9</sup>對應 = Match

可以證明 PCP 是一個不可判定的語言。

### 3.2 使用 PCP 做計算

給定一個圖靈機  $M$ ，我們可以設計出一組特別的骨牌  $P$ ，使得在解 PCP 的過程中，骨牌排出的字串模擬了圖靈機的運算過程。

以下以舉例的方式說明用 (M)PCP 模擬計算的方法。令  $M$  為一台「只接受 01 並改寫為 10」的圖靈機。我們可以給出它的轉移函數  $\delta$ ，以供設計骨牌時參考。

$$\begin{cases} q(q_0, 0) = (q_1, 1, R) \\ q(q_1, 1) = (q_{\text{accept}}, 0, R) \\ q(q, x) = (q_{\text{reject}}, -, R) \text{ otherwise} \end{cases}$$

依據教科書 [1] 第 229 頁所述之骨牌設計方式， $P$  包含下列骨牌。

- Part 1:  $\left[ \frac{\#}{\#q_0 0 1 \#} \right]$
- Part 2:  $\left[ \frac{q_0 0}{1 q_1} \right], \left[ \frac{q_1 1}{0 q_{\text{accept}}} \right]$
- Part 3: 此圖靈機無向左移動的可能，故不適用。
- Part 4:  $\left[ \frac{0}{0} \right], \left[ \frac{1}{1} \right]$
- Part 5:  $\left[ \frac{\#}{\#} \right], \left[ \frac{\#}{-\#} \right]$
- Part 6:  $\left[ \frac{0 q_{\text{accept}}}{q_{\text{accept}}} \right], \left[ \frac{q_{\text{accept}} 0}{q_{\text{accept}}} \right], \left[ \frac{1 q_{\text{accept}}}{q_{\text{accept}}} \right], \left[ \frac{q_{\text{accept}} 1}{q_{\text{accept}}} \right]$
- Part 7:  $\left[ \frac{q_{\text{accept}} \# \#}{\#} \right]$

以  $\left[ \frac{\#}{\#q_0 0 1 \#} \right]$  作為開頭，則一開始我們會得到上下不相等的骨牌：

$$\left[ \frac{\#}{\#q_0 0 1 \#} \right]$$

注意紅色的部分以  $q_0 0$  開頭。若我們想要上下相等的字串，則需要上半部以  $q_0 0$  開頭的骨牌作為下一張骨牌。在  $P$  中，這樣的骨牌只有一張，故我們得到：

$$\left[ \frac{\#}{\#q_001\#} \right] \left[ \frac{q_00}{1q_1} \right]$$

按照相同的邏輯，在每個步驟我們都尋找  $P$  中符合目前「多出來」的字串的骨牌，依序排上，則最後可以得到：

$$\left[ \frac{\#}{\#q_001\#} \right] \left[ \frac{q_00}{1q_1} \right] \left[ \frac{1}{1} \right] \left[ \frac{\#}{\#} \right] \left[ \frac{1}{1} \right] \left[ \frac{q_11}{0q_{\text{accept}}} \right] \left[ \frac{\#}{\#} \right] \left[ \frac{1}{1} \right] \left[ \frac{0q_{\text{accept}}}{q_{\text{accept}}} \right] \left[ \frac{\#}{\#} \right] \left[ \frac{1q_{\text{accept}}}{q_{\text{accept}}} \right] \left[ \frac{\#}{\#} \right] \left[ \frac{q_{\text{accept}}\#\#}{\#} \right]$$

注意藍色部分以井字號  $\#$  分隔，對應到的即是  $q_001 \vdash 1q_11 \vdash 01q_{\text{accept}}$  的計算；後方冗餘的項只是因應上下對應所需。

在這個例子中為了舉例方便，我們使用了 MPCP 版本，亦即第一張骨牌被指定為  $\left[ \frac{\#}{\#q_001\#} \right]$ 。若要使用 PCP 來進行計算，則需要事先在每張骨牌上插入一些  $\star$  字符，用以強迫任何對應必須要以該骨牌開頭。

## 引用

- [1] M. Sipser, *Introduction to the theory of computation, third edition*. Cengage, 2013.
- [2] W.-K. Hon, "Lecture notes in theory of computation." 2007.