# 一道密碼算術謎題的啓示

【文 / 課程及教學研究中心副研究員 葉家棟】

紐厄爾與賽蒙（Newell & Simon, 1972）在研究人類問題解決時，使用一種密碼算術謎題（a cryptarithmetic puzzle）作爲研究工具。他們記錄下解題者演算的每一步驟，並且根據這些資料，探討人類如何有效的解決問題。什麼是密碼算術謎題？它是一種以英文字母進行運算的謎題，其解題的目標是將英文字母換成數字（0－9）。例如：

$$\begin{array}{r} \text{S E N D} \\ +\quad \text{M O R E} \\ \hline \text{M O N E Y} \end{array}$$

要求包括：（1）把英文字母換成數字 0－9；（2）每一個英文字母代表一個不同的數字；（3）在英文字母組中，第一個英文字母不能爲 0；（4）英文字母換成數字後，下面一行數字的答案必須等於第一行和第二行之和。

要解決這個問題，運用隨機嘗試（trial and error）的方法，是很難得出正確答案的。因爲解題共有 $\frac{10!}{2!} = 2 \times 10^6$ 次可能的嘗試，在此題，由任何兩個四位數字相加的和必定小於 20000 的數學知識，可推論得 M＝1，則可能的嘗試減爲 $\frac{9!}{2!} = 2 \times 10^5$ 次。運用隨機嘗試的方法，就是對每個英文字母任意對應一個數字，進行計算。當發生矛盾時，就把數字和英文字母的對應關係再作新的安排，重新計算。如指定 S＝9，E＝5，N＝6，D＝7，M＝1，O＝3，R＝8，Y＝2，但是，當計算到 N＝E＋O＋1（進位）＝5＋3＋1＝9，而不是 6 時，就知道錯了。這時就需要重新指定數字代替英文字母，再作計算。這種隨機嘗試的方法，需要 $2 \times 10^5$ 次，才能找到正確的答案。

另一種方法是系統地從右向左，充分利用解決問題中所獲得的知識。由任何兩個四位數字相加的和必定小於 20000 的數學知識，可推論得 M＝1。由於已知 M 的數值，嘗試的範圍就縮小了。由於最右邊第 1 行沒有提供任何信息，因此必須嘗試著加以解決。假設 D＝7 及 E＝8，可推論得 Y＝5。由於第 2 行沒有提供任何信息，因此也必須嘗試著加以解決。假設 N＝6，可得 R＝1。這個 R＝1 的結果與已知 M＝1 矛盾，所以 D＝7、E＝8 及 N＝6 的假設是錯誤的。運用這種方法反覆試驗，經過多次組合，可以得出一個正確答案。

然而這兩種方法—隨機嘗試和系統嘗試，都不是有效解決算術密碼謎題的方法。如何有效解決算術密碼謎題？

根據紐厄爾與賽蒙的解題策略，解題從可能性最少的一行，就是限制性最多的那一行開始。例如，此題從左側開始：

第 1 行：由任何兩個四位數字相加的和必定小於 20000 的數學知識，可推論得 M 可能是 0 或者 1；這個 M =0 的結果與第一個英文字母不能爲 0 的題設要求矛盾，所以 M 不可能是 0，M 必定是 1；問題可簡化爲：

$$\begin{array}{r} \text{SEND} \\ +\quad \text{1ORE} \\ \hline \text{1ONEY} \end{array}$$

第 2 行：有兩種可能性，（1）假設沒有第 3 行進位的 1，則 $S+1 \geq 10$，由 $S+1=10+O$ 的關係式，可推論得 S 可能是 9，O 可能是 0；（2）假設有第 3 行進位的 1，則 $S+1+1$（進位）$\geq 10$，由 $S+1+1$（進位）$=10+O$ 的關係式，可推論得 S 可能是 8 或者 9，O 可能是 0 或者 1，這個 $O=1$ 的結果與 $M=1$ 的結果矛盾，所以 O 必定是 0；第 2、3 行的英文字母 O 可置換成數字 0；問題可簡化爲：

$$\begin{array}{r} \text{SEND} \\ +\quad \text{10RE} \\ \hline \text{10NEY} \end{array}$$

第 3 行：由任何數字與 0 相加的和必定小於 10 的知識，可得兩種可能性，（1）假設沒有第 4 行進位的 1，由已知 $E+0<10$，及 $E+0=N$ 的關係式，可推論得 $E=N$，這個 $E=N$ 的結果與每一個英文字母代表一個不同的數字的題設要求矛盾，所以這個假設是錯誤的；（2）假設有第 4 行進位的 1，由已知 $O=0$，$E+0<10$，及 $E+0+1$（進位）$=N$ 的關係式，可推論得 $E+1=N$；問題無法再簡化，由於獲得第 3 行的計算結果小於或等於 9 的信息，回到第 2 行。

第 2 行：由已知沒有第 3 行進位的 1 的信息，及已知 $S+1 \geq 10$，可推論得 $S=9$，問題可簡化爲：

$$\begin{array}{r} \text{9END} \\ +\quad \text{10RE} \\ \hline \text{10NEY} \end{array}$$

第 4 行：由已知有第 4 行進位的 1 的信息，可得兩種可能性，（1）假設沒有第 5 行進位的 1，由已知 $N+R \geq 10$，$N+R=10+E$ 的關係式，及已知 $E+1=N$ 的信息，可推論得 $R=9$，這個 $R=9$ 的結果與 $S=9$ 的結果矛盾，所以這個假設是錯誤的；（2）假設有從第 5 行進位的 1，由 $N+R+1$（進位）$\geq 10$，$N+R+1$（進位）$=10+E$ 的關係式，及已知 $E+1=N$ 的信息，可推論得 $R=8$；回到第 3 行，問題可簡化爲：

$$\begin{array}{r} \text{9END} \\ +\quad \text{108E} \\ \hline \text{10NEY} \end{array}$$

第 3 行：現在只剩下六個數字 7、6、5、4、3 及 2 和四個英文字母 E、N、D 及 Y，由已知 $E+1=N$ 的信息，可推論得 E 不可能是 7；問題無法再簡化。

第 5 行：由已知有從第 5 行進位的 1 的信息，可推論得 $D+E \geq 10$，由剩下六個數字 7、6、5、4、3 及 2，可推論得 $D \leq 7$，由 $D+E=10+Y$ 的關係式，已知 $M=1$，及已知 $O=0$，可推論得 $E>4$；由已知 E 不可能是 7，可推論得 E 可能是 5 或者 6，D 可能是 4 或者 5 或者 6 或者 7；有兩

種可能性，（1）假設 E = 5，由已知 N = E + 1，可推論得 N = 6，由已知 D + E = 10 + Y 關係式，可推論得 D＞6，所以 D = 7，Y = 2；（2）假設 E = 6，由已知 N = E + 1，可推論得 N = 7，由已知 D + E = 10 + Y 關係式，可推論得 D＞4，所以 D = 5，Y = 1，這個 Y = 1 的結果與 M = 1 的結果矛盾，所以這個 E = 6 的假設是錯誤的；所以 E = 5，N = 6，D = 7，Y =2；最後結果爲：

$$\begin{array}{r} 9567 \\ +\quad 1085 \\ \hline 10652 \end{array}$$

張義生（2009）將密碼算術謎題歸類爲一種信息不充分問題。這種問題的特徵就是解題者所掌握的關於解題的信息不完全，使用這些信息不能夠直接地解決問題。紐厄爾與賽蒙根據這種問題的特徵，提出盡可能縮小問題空間的解題策略。在解題時，運用該解題策略的具體方法包括：

充分利用已知信息。面對需要解決的問題時，充分利用解題者已有的經驗、知識和問題提供的全部信息，包括解題的目標、實現該目標的相關要求及現有的條件，找出可能性最少（或限制性最多）的環節，作爲解題的起點。

盡可能擴充信息。解題從最容易的環節開始，例如先找出謎題可能性最少（或限制性最多）的一行，從中獲得最多的信息，再利用已有的經驗、知識進行推理，盡可能縮小問題空間，直到找到正確的答案。

簡化問題。在擴充信息的過程中，進行問題的簡化，例如以已知數字置換謎題的英文字母，可明確掌握解題的目標、實現解題目標的相關要求及現有的條件的變化，並可避免重複解題步驟。

參考文獻

張義生（2009）：**求解思維的邏輯**。合肥：安徽大學出版社。

Newell, A., & Simon, H. A. (1972). Human problem solving. Englewood Cliffs, NJ: Prentice-Hall.