行政院國家科學委員會專題研究計畫　成果報告

量子自動機之計算能力研究

計畫類別：個別型計畫
計畫編號：NSC92-2218-E-002-053-
執行期間：92 年 12 月 01 日至 93 年 10 月 31 日
執行單位：國立臺灣大學電機工程學系暨研究所

計畫主持人：顏嗣鈞

計畫參與人員：彭柏源、 何明彥、 吳國勝

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 94 年 2 月 1 日

行政院國家科學委員會專題研究計劃成果報告

量子自動機之計算能力研究

計畫編號: 92-2218-E-002-053
執行期間:92 年 12 月 1 日至 93 年 10 月 31 日
計畫主持人: 顏嗣鈞 教授 國立台灣大學電機工程系
計劃參與人員: 彭柏源、 何明彥、 吳國勝

一、摘要

在探討古典的計算理論相關議題時，通常會試著提出某種計算模型來與有限自動機、堆疊自動機、或涂林機等典型的模型作問題的可計算性以及解決問題所需資源的複雜度的比較。我們所關心的*迴轉次數限制多計數器自動機*，係一個計算能力與堆疊自動機之間處於模糊地帶的自動機類型。本計畫的目的是試圖去完成此計算模型的量子自動機的正規定義，並舉出其所能接受的例子，進而與其他模型作比較。此外，*盲多計數器自動機*的能力與迴轉次數限制多計數器自動機的能力無異，因此發展並比較此二模型的量子自動機也是我們所感興趣的研究議題。

關鍵字： 多計數器自動機、迴轉次數限制、盲多計數器自動機、量子自動機。

In this project, the quantum version of a computational model called “reversal-bounded multi-counter automata” is considered. The goal of this project is to provide the formal definition of the model, propose some examples accepted by such automata, and furthermore compare their computational power with others’. In addition, two quantum versions of the so-called blind counter machines are also investigated.

Keyword: Multicounter machines, reversal-bounded, (partial) blind multicounter machines, quantum automata.

二、計畫緣由與目的

古典的計算理論所探討的問題一般而言被分為下列兩個構面：

- 計算模型對於不同問題的*可計算性* (computability)；
- 計算模型解決不同的可計算問題，對於資源量需求的*複雜度*(complexity)。

就問題的可計算性而言，大多數人所考慮的計算模型的典型，通常以有限自動機 (finite automata)，堆疊自動機(push-down automata ）以及涂林機 (Turing machines) 為三個計算能力分級的代表：有限自動機與堆疊自動機可以決定的輸入形式，正好分別對應了在正規語言學上的*正則語言* (regular languages) 和*語境自由語法* (context-free grammar)；而涂林機的計算模型，根據 Church & Turing 的研究，可以認定為問題可計算性的判斷標準，也就是可以被論證的命題，即可以被涂林機所決定 (此即所謂*丘奇-涂林論點* Church -Turing thesis)。就可計算問題對於資源量需求的複雜度而言，大多數的研究著重於涂林機在限制時間需求以及/或者空間需求的情形下，問題的可計算性。由於涂林機具有常數倍數時間/空間等效的特性 (linear speed-up theorem 以及 tape compression theorem)，甚至長久以來，所謂的*延伸丘奇-涂林論點*（extended Church-Turing Thesis）認定可以用物理定律構造的計算工具所需要花多項式時間所解決的問題均可以使用涂林機在多項式時間內解決；一般而言，當我們在討論可計算問題的資源量的複雜度時，都將複雜度分成對數等級，多項式等級，以及指數等級。

本計畫所關心的計數器自動機(counter automata)，根據其計數器個數的不同，而有截然不同的計算能力——僅具有一個計數器的計數器自動機，其計算能力略遜於堆疊自動機；然而，具有二個以上計數器的計數器自動機，在不限制計算時間與空間的情形下，其計算能力與涂林機無異。若對於多計數器自動機作各種不同的時間或空間上限制時，則其能力也會有所不同。Ibarra [4] 在 1978 年提出所謂的迴轉次數限制多*計數器自動機*（reversal-bounded multi-counter machines）。*(m, n)迴轉次數限制 k 計數器自動機*（(*m*,*n*)-reversal-bounded *k*-counter machines）則為一個讀取頭可以來回移動次數最多 m 次，且每個計數器可以來回計數最多 n 次；在確定性的運作模式下自動機的類別為 DFCM(k, m, n)，而在非確定性的運作模式下自動機的類別為 NFCM(k, m, n)。

通常多計數器自動機的行動是根據輸入的符號（input symbol）、自動機的狀態（state）、和每個計數器的符號（sign of each counter）所決定的。當一個多計數器自動機在沒有給各個計數器的符號或大小的資訊也可以行動時，則被稱為*盲多計數器自動機*（blind multicounter machines）。其能力並沒有因限制而變得毫無能力，[3] 證明其能力與迴轉次數限制多計數器自動機一樣強。另外，當一個盲多計數器自動機的每個計數器均被限制為非負的整數時，則稱為*部分盲多計數器自動機*（partial blind multicounter machines）。雖然限制增加了，不過由於它多知道了計數器必非負的資訊，所以其能力較盲多計數器來得強。

相較於古典計算理論，由於量子物理的發展，古典的計算理論中所謂「不是這樣就是那樣」的布林代數的觀念將無法套用在以量子物理為基礎的資訊系統。為此，近十數年來發展出的所謂量子計算理論的觀念，成為描述量子計算模型的主要數學工具。在量子計算理論中，任意確定的狀態均為一個量子系統一個基本的面向，而當我們對於這個系統進行一個特定的操作時，會將這個系統的狀態推展成為眾多*不同基本狀態的疊加*。而這些系統狀態的疊加，乃是依循線性代數的計算模式，也就是當我們對此系統進行一個操作時，從數學上的觀點來看，其實是對於這個系統施以一個固定長度矩陣（unitary matrix）的運算，而將系統的狀態投射到所有基本狀態所構成的向量空間（又可稱為希爾柏特空間 Hilbert space）上。

在量子計算理論中另一個被關注的焦點是*量測*（measurement）。由於我們在量子系統運算的過程中，該系統的狀態被投射成不同基本狀態的疊加，然而當我們真正地進行量測時，該系統的狀態會被簡化成所有可能基本狀態中的一種，並且一旦我們進行量測，被量測出來的系統狀態會被鎖定，因此之後的運算只會依照該系統原先在被量測到的狀態來進行。因此在計算的過程中，僅僅在計算結束之後進行量測，以及在計算的過程中就進行量測，其計算能力可能有所不同。

在本計畫中，我們關心的是較低階的

量子計算模型的一些問題。這類型問題的典型是，將有限自動機加入量子的觀念，形成所謂量子有限自動機（quantum finite automata），接著討論在量測一次（measure-one）以及量測多次（measure-many），在自動機讀取頭單向移動（one-way）以及雙向移動（two-way）的情形下，量子有限自動機的行為。Kondacs & Watrous 在 1997 年證明了一個量測一次但雙向移動的量子有限自動機可以在僅有單邊誤差的情況下，準確接受某些語境自由語法所描述的語言，甚至接受某些連語境自由語法也無法描述的語言。

三、計畫方法

在量子計算理論中，我們討論量子計算模型的基本原則是，將古典計算理論提到的各種計算模型中，所有與狀態變動有關的面向，由原先布林代數「非此即彼」的觀念，全部改成量子計算模型中的狀態疊加的觀念，然後由這樣的觀念出發，藉以探討下列三種計算模型上的變化：

1. 所產生的量子計算模型，其在量測一次或者量測多次的情況下，與古典計算理論的模型相比較，所接受的語言的變化。
2. 所產生的量子計算模型，是否具有可程式性，亦即是否存在有一個該模型的特例，使得我們可以輸入其他相同模型的描述，而使得該特例能夠模擬輸入的模型。
3. 所產生的量子計算模型的一些相關判定性問題是否為可決定。

相關量子計算模型的討論始終脫離不了兩個面向，其一為將涂林機的計算模式加入量子計算的狀態疊加的觀念，發展出來的量子涂林機（quantum Turing machines），對於問題的可計算性，以及不同的量子可計算性問題的時間與空間複雜度的需求；其二為將古典計算理論中計算能力未及涂林機的計算模型加入量子計算的狀態疊加的觀念，而由其中討論加入量子概念之後問題在這些計算能力較低的量子計算模型上的可計算性──其中也包括了一些與該模型本身相關的問題的可判定性。另外，由於量子計算模型的狀態乃是以基本狀態疊加的方式所造成，而所疊加的各種基本狀態可以是接受的狀態或者拒絕的狀態，因此我們討論量子模型是否接受一個語言時，經常性地將接受的機率一併考慮──甚至在古典計算理論中討論*機率涂林機*（probabilistic Turing machines）時考慮的有限失誤（bounded-error）以及無限失誤（unbounded-error）的情形，在量子模型中經常性地一併觀察。

相較於 QFA 而言，其他關於計算能力低於涂林機的計算模型，加入量子計算的觀念之後得到的計算模型的能力，文獻就相對較少並且零散，但是建立模型的基本方法和 QFA 相同：

1. 將古典計算模型中資訊基本單位──位元改為量子位元，據以提出一個量子版本的計算模型。
2. 檢查計算模型中的完整構成條件，以確保在量子系統中，所有和觀察無關的操作在數學的觀點來看都是固定長度矩陣。
3. 倘若該種量子計算模型，必須考慮一次觀察或多次觀察，讀 (寫) 頭單向或雙向，以及有限誤差或無限誤差的問題時，設法加以討論其差別。
4. 比較該種量子計算模型與已知的其他計算模型 (包括古典或者量子) 之間的差異性。

四、結論與未來展望

本計畫完成後，會持續探討量子迴轉次數

限制多計數器自動機的定義，並且能夠舉出某些不明顯但可以被這種計算模型所接受的例子，以反映出這種計算模型的特性。對於這種計算模型與各種不同的其他(包括古典或者量子) 計算模型之間的關聯加以探討，預期最終貢獻乃是在於將這個模型與其他模型的關聯加以嚴格界定，藉此能夠確實反映出這個計算模型的特徵，以期當我們討論其他的計算模型時，可以利用這個模型作為評比計算能力的標準。此外，古典的盲多計數器自動機的能力與迴轉次數限制多計數器自動機無異，因此比較此二模型的量子自動機的能力也是相當地重要。

對於學術研究、國家發展及其他應用方面預期之貢獻，本計畫由於乃是針對某特定之古典計算模型加入量子計算的觀念之後加以探討，一方面對於國內量子計算的理論研究注入競爭力，另一方面可能隨之產生的數學工具對於相關計算理論的學術研究也可能有很大的助益。至於應用方面，若在定義計算模型時可注意到實作上的可能性，則理論反映了實際情形，所得到的理論事實可以反映在實作上，對於實務應用也會有相當大的幫助。

由於本計畫一方面對於早期的計算理論相關文獻加以整理，另一方面則是定義出新的計算模型並加以探討，參與的人員不僅對於早期的計算理論相關成果會有更為深入的了解，在參與本計畫之後也會對於如何定義一個新的數學模型，並且藉由該數學模型加以分析推導有清晰的概念。

五、參考文獻

[1] A. Brodsky and N. Pippenger, "Characterizations of 1-Way Quantum Finite Automata," *SIAM Journal on Computing*, Vol. 31(5), pp. 1456-1478, 2002.

[2] S. Greibach, "Remarks on blind and partially blind one-way multicounter machines," *Theoretical Computer Science*, Vol. 7, pp. 311-324, 1978.

[3] O. Ibarra, "Reversal-bounded multicounter machines and their decision problems," *J. ACM*, vol. 25, no. 1, pp. 116-133, 1978.

[4] A. Kondacs and J. Watrous, "On the power of quantum finite state automata," *Proceedings of FOCS'97*, pp. 66-75, 1997.

[5] M. Kravtsev, "Quantum finite one-counter automata," *Proceedings of SOFSEM'99*, Lecture Notes in Computer Science, Vol. 1725, pp. 431-440, 1999.

[6] C. Moore and J. Crutchfield, "Quantum Automata and Quantum Grammars," *Theoretical Computer Science*, Vol. 237(1-2), pp. 275-306, 2000.