行政院國家科學委員會專題研究計畫　期中進度報告

量子計算機之系統架構研究與設計(1/3)

計畫類別：個別型計畫
計畫編號：NSC93-2218-E-002-098-
執行期間：93 年 08 月 01 日至 94 年 07 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：郭斯彥

計畫參與人員：蔡一鳴、盧勤庸、王秀安、王瀚偉

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 5 月 24 日

行政院國家科學委員會補助專題研究計畫 □ 成 果 報 告 ■期中進度報告

量子計算機之系統架構研究與設計

計畫類別：■ 個別型計畫　　□整合型計畫
計畫編號：NSC－93－2218－E－002－098
執行期間：93 年 8 月 1 日至 94 年 7 月 31 日

計畫主持人：郭斯彥

計畫參與人員：蔡一鳴、盧勤庸、王秀安、王瀚偉

成果報告類型(依經費核定清單規定繳交)：■精簡報告 □完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
■出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立台灣大學 電機工程學系

中　華　民　國　94　年　5　月　23　日

行政院國家科學委員會專題研究計畫成果報告
量子計算機之系統架構研究與設計

A Study and Design on the Architecture of Quantum Computers

計畫編號：NSC 93-2218-E-002-098
執行期限：民國93年08月01日到94年07月31日
主持人　：郭斯彥　台灣大學電機工程學系教授

一、中英文摘要

自從量子電腦的概念於 1980 年代初期被提出後[1-3]，量子資訊科學便成為一門相當新而發展快速的研究領域。本計劃由量子電路的觀點研究量子計算系統之架構，同時以核磁共振(Nuclear Magnetic Resonance, NMR)之技術實作一個量子計算系統。

要實作完成一部量子電腦，發展一套有效的量子電路合成方法是有必要的。量子電路的基本元件是量子位元，因為量子位元製作不易，所以合成出來之量子電路需要具有較低成本和較容易實作的特性。本計劃中，我們使用表格式演算法發展出一個量子布林電路化簡方法，這個方法可以同時地執行 AND 和 XOR 函數化簡，當一個量子布林電路被化簡後，我們還必須驗證化簡後的電路與原來電路有相同的功能。

在有了量子電路合成的工具之後，本計劃選擇使用核磁共振的方式來實作一個量子計算系統。我們利用基於碳的同位素碳 13 之三氯甲烷(chloroform)中的 ^{1}H 和 ^{13}C ($^{13}CHC1_3$)做為資訊的承載單位，NMR RF 脈衝用來操控其中之量子狀態，以實現一個 2 位元的 NMR 量子計算系統雛形。值得注意的是，只要承載資訊的單位(量子位元)可以根據量子力學的方式進行操作，一個量子計算系統獨立於底層的實作技術，並不因其改變而受影響。

關鍵詞：量子計算，量子通信，量子電路，電路合成，電路檢測，核磁共振技術。

Abstract

The study of quantum information science has expanded rapidly since the theoretical model of quantum computers were introduced in the early 1980's [1-3]. In this project, we study the architecture of quantum computing systems from the circuit point of view and demonstrate physical implementations using nuclear magnetic resonance (NMR) technology.

To implement a quantum computer, it is necessary to develop an efficient quantum circuit synthesis method. Since the quantum bit (which is the basic component of a quantum circuit) is very expensive, a good quantum circuit has to be designed in a cost-effective way and, at the same time, it must be easy for implementation. In this project we describe a simplification method of quantum Boolean circuits using a tabulation algorithm. This method performs AND and XOR function simplification simultaneously. After a quantum Boolean circuit is simplified, we verify the circuits to confirm its function is correct.

With the capability of performing quantum circuit synthesis, we report an experimental realization of quantum switch using nuclear spins and magnetic resonant pulses in this project. The nuclear spins of ^{1}H and ^{13}C in carbon-13 labeled chloroform are used to carry the information. Then nuclear magnetic resonance pulses are applied to perform quantum operations on a two-qubit quantum computer prototype. Note that, an ideal quantum computation system is independent of the underlying physical

implementation, as long as the information carrier (qubit) can be manipulated according to quantum mechanics.

Keywords: Quantum Computing, Quantum Communications, Quantum Circuits, Circuit Synthesis, Circuit Testing, Nuclear Magnetic Resonance (NMR).

二、前言

量子資訊科學是一門相當新的研究領域，自從1994 年量子演算法被發現可以用來在多項式時間內解出因數分解以及離散對數的問題後，有關量子計算、量子通訊的研究便疾速增加，也開始吸引大量研究經費的投入，目前在美國、歐洲、日本以及中國大陸，已經有許多專為此新領域而成立的研究團隊或研究機構。雖然目前具有幾個量子位元的量子電腦已有初步成果，多量子位元的量子電腦仍在設計與實驗中。也正由於世界各先進國家對量子計算及量子通信之發展尚處於實驗階段，本計劃之執行便也格外顯得前瞻而具有國際競爭性。

三、研究目的

本子計畫擬對量子電路之合成、測試、以及量子系統之實作方式做一深入研究，以期能帶動國內量子資訊科學的研究風氣。其內容與成果包括量子電路合成及測試之理論分析，演算法探討，以及如何使用核磁共振的方式來製作一個量子計算系統的實作過程。

四、文獻探討

量子電腦的概念最先是於1980年代初期被提出的 [1]-[3]，從那時開始便有許多學者紛紛投入這個領域的研究。在安全金鑰傳遞 [4]、多項式時間分解質因數 [5] 以及快速資料庫搜尋演算法 [6] 等應用紛紛出現後，量子資訊有了很大的進展，這些結果使得量子資訊科學在最近成為發展最快速的研究領域。另外，其他方面如量子電路的合成以及各種量子計算機的實作技術，包括離子井[8]、光學腔[9]、核磁共振[10]、量子點[11]以矽基解決方案[12]等等，都讓這個領域更加接近實際應用的階段。

五、研究方法

本研究之整體目的在於對量子電路以及量子系統之實作方式做一深入研究。想要達成實作量子計算系統的目的，必須先就量子電路的合成及測試等子目標著手。所以，本計劃之研究方法包含先分析及解決下述之子目標。子目標一是我們必須設計一個多變數的量子布林電路化簡方法，這個方法要可以化簡多變數的量子布林邏輯函數。當電路化簡之後，我們還需要驗證測試化簡的量子布林電路是否和原來電路有等效的作用，這個方法就是函數驗證。所以，本研究之第二個子目標在於提出一個驗證測試化簡的量子電路的方法。最後，基於以上之研究，我們便可利用對量子電路的瞭解來架構一部核磁共振量子電腦，並利用 RF 脈衝來實作操控它所需要之量子作用。接下來，我們便描述研究這些階段性目標的一些結果。

六、結果與討論

在本計劃中我們分別先由量子電路之合成及檢測來研究量子計算之系統架構。在量子電路合成方面，為了要完成量子電腦，我們必須建立量子布林電路，這些電路是由量子邏輯閘組成的，不像傳統的 AND-OR-NOT 電路，量子布林電路是以 NOT、CN 和 CCN 閘當成基本元件，雖然有一個不同的基本邏輯閘，電路仍然可以使用傳統 AND、XOR 和 NOT 函數進行電路合成。

在本計劃中，我們提出了一個表格式演算法，表格式演算法可以用來簡化布林函數，特別是針對較多的變數的情況，這個演算法的概念有兩個優點，分別說明如

下:

1) 這個演算法可以程式化，以做為量子布林電路的化簡工具。
2) 對於量子布林電路的化簡，這個方法是一個非常有前景的技術。

本表格式演算法是利用列表方式，分別針對 AND 和 XOR 函數進行化簡，在每一個週期，可以找到一個最簡化的項目，這個項目具有最多的 1，並且可以產生一個部份方程式，最後組合這些部份方程式，就可以到化簡結果。假設原來的真值表有 n 個變數，這個演算法的說明如下:

1. 計算 1 的數目，如果超過 2^{n-1}，則更改 1 為 0，0 更改為 1。
2. 對 1 進行分組。
3. 執行 AND 函數產生。
4. 執行 XOR 函數產生。
5. 從上面步驟 3 和 4 中，選擇最簡化的項目，根據所選的項目，可以得這個項目的布林函數，接下來，更改這個項目中的 1 為 0，0 更改為 1。
6. 如果仍然有 1 存在，則跳到步驟 2。
7. 最後，組合所有布林函數。

至於在量子電路檢測方面，我們也提出了電路測試演算法，在這個演算法中，利用由後向前傳遞方式找到一組測試向量。輸入這組向量到電路中，檢查輸出向量是否正確，可以利用測試結果找到有問題的量子位元。假設 n 個位元的量子布林電路有 m 個量子邏輯閘，這個演算法的說明如下:

1. 掃描整個電路，並且記錄每一個目的量子位元的位置。
2. 選一個未標示的量子位元，這個位元是某個邏輯閘的目的量子位元，然後標示這個位元。
3. 利用由後向前傳遞方式，找到測試方程式。
4. 根據測試方程式，可以得到一組測試向量。
5. 如果仍然有未標示的量子位元，則跳到步驟 2。
6. 組合所有測試向量，可以得到一組必要測試向量。
7. 輸入必要測試向量到電路中，並且找到具有不正確值的輸出量子位元。
8. 根據錯誤量子位元的位置，可以找到故障閘的可能位置。

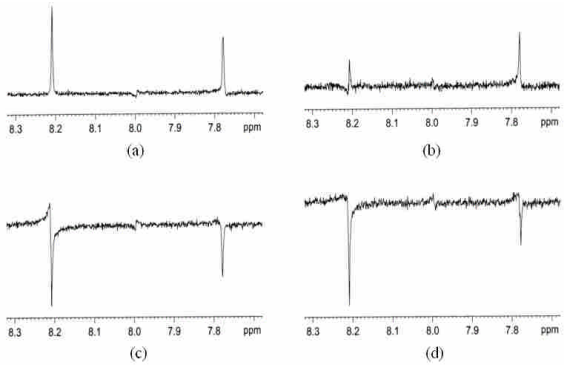
在有足夠的技術能合成及檢驗量子電路之後，便可以開始著手實作量子計算系統。最近幾年來量子實際製作方法的進展十分地迅速，，讓科學家有許多不同方法可以實現量子力學的應用。在這些解決方案中，核磁共振是一項比較成熟的技術，在化學和醫學領域中也已經有了廣泛的應用。在許多報告中也證明了 NMR 能夠實作量子計算系統，並且解決傳統計算所無法解決的問題。本計劃選擇使用核磁共振的方式來實作量子計算系統，利用基於碳的同位素碳 13 之三氯甲烷(chloroform)中的 ^{1}H 和 ^{13}C ($^{13}CHC1_3$)做為資訊的承載單位，實現 2 位元的 NMR 量子計算系統之雛形。值得注意的是，只要承載資訊的狀態可以根據量子力學的方式進行操作，一個量子計算系統其實是不受限於底層的技術。

量子計算機中最重要的動作就是兩個(或多個)量子位元之間的互相作用。兩個量子位元的條件式邏輯可以透過自旋交互作用(spin-spin coupling)的效果來達成，本計劃中，自旋交互作用是 ^{1}H 和 ^{13}C 自旋狀態之間的互動結果，以 Hertz (Hz)為單位來量測。由於這個偶合關係，一個量子位元的進動就可以根據其他量子位元的狀態增加或減少。如果在脈衝波順序中加入某些特定的自由演化(free evolution)時間，目標量子位元的狀態就可以依據控制量子位元的狀態條件式的進行相位移轉。這基本上就是一個控制-相位轉移(control-phase-shift)閘，它也可以用來產生其他量子條件式邏輯閘。**CN** 閘是兩個量子位元條件式邏輯閘的其中一個範例，**CN** 閘可以分解成兩個 **H** 閘和一個 π 角度的控制-相位轉移閘。

在實驗方面，我們將 $^{13}CHC1_3$ 置於室溫中的 d6-Acetone 來做為此交換器之平台，利用其中的 ^{1}H 和 ^{13}C 原子來承載資訊。實驗的脈衝波能量在頻道 1 (^{1}H)中設為 3.00 dB，在頻道 2 (^{13}C)中則設為-3.00 dB。對頻道 1 的 90 度脈衝波時間為 9.5 μs，頻道 2 則為 12.6 μs。因為單一量子位元操作的旋轉角度跟能量和 RF 脈衝波的時間成正比，所以經過簡單的計算就可以得到 45 度和 180 度脈衝波的時間。在自旋交互作用控制下的自由演化是量子計算中條件式邏輯的來源，^{1}H 和 ^{13}C 之間的自旋交互作用量測結果為 215 Hz。因此，計算之後 90 度的自由演化時間為 1.165 μs，180 度旋轉則需 2.33 μs，剛好是 90 度旋轉的兩倍。這些參數都必須指定到 Bruker 脈衝波程式中的 D、P 以及 PL 陣列。

在 NMR 的實驗中通常需要執行多次相同的掃描，以便改善其雜訊比(signal to noise ratio)，這個掃描的次數稱為 NS (Number of Scans)。在標準的化學實驗中，典型的 NS 值通常介於 1000 到 10000 之間，依據樣本的密度而定。另外，為了讓樣本達到穩定狀態，在實際的脈衝波之前必須先試幾個試驗的脈衝波，這個時候不用收集它的 NMR 訊號。這個參數稱為 DS (Dummy Scans)，DS 值通常介於 4 到 8 之間。因為本實驗使用了濃縮的樣本，所以 NS 與 DS 參數分別設為 8 和 0。其他必要的參數還有時間域(Time Domain size, TD)的大小，它是用來指定時間軸上欲收集資訊的時間點總數；以及 FID Resolution (FIDRES)，用來指定每個點之間的頻率範圍。本實驗的 TD 設為 32k，FIDRES 則設為 0.305176 Hz。結果若以 10000 Hz 的 Spectral Width (SW)做觀察，需要時間大約為 1.63845 秒。

本計劃利用國科會貴儀中心之 Bruker Avance DMX-500MHz NMR 系統，將 $^{13}CHC1_3$ 置於室溫中的 d6-Acetone 來做為此交換器之平台，利用其中的 ^{1}H 和 ^{13}C 原子來承載資訊。實驗中我們將頻道 1 設為 ^{1}H，頻道 2 設為 ^{13}C，由此觀察連續三個量子位元互動(**CN** 閘)的作用。在收集資料與後續處理(尤其是相位修正)之後，連續三個量子位元互動(**CN** 閘)的作用如圖一所示。圖中顯示了正確的 CN 閘的動作。由於 CN 閘是一個基本閘，它與單量子位元旋轉可以組成任何量子操作，故而就理論上而言，我們已經可以達成操控 NMR 量子電腦的結果了。



圖一、NMR 量子計算機連續執行 CN 閘後的結果

本年度至目前討論的結果為止完成之工作項目包含下列各項：

1. 量子電路合成之理論與演算法
2. 量子電路測試之理論與演算法
3. 以核磁共振的方式來實作 2 位元之量子計算系統

下年度之計畫預計將研究如何利用 NMR 量子計算系統來實現量子演算法，其目標如下：

1. 量子演算法之理論與設計
2. 量子演算法於 NMR 量子計算系統之實作
3. NMR 量子計算機之脈衝程式編譯器
4. 多位元 NMR 量子計算系統之實作

如果以上目標皆順利達成，預計可激勵並帶動國內量子計算領域之研究，使得量子計算與通信之相關產業更易於早日到來。

七、參考文獻

[1] P. Benioff, “The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing

machines," J. Stat. Phys., vol. 22, no. 5, pp. 563–591, 1980.
[2] R. Feynman, "Simulating physics with computers," Int. J. Theor.Phys., vol. 21, pp. 467–488, 1982.
[3] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," in Proc. R. Soc. Lond. A, vol. 400, 1985, pp.97–117.
[4] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Computers Systems and Signal Processing, 1984, pp. 175–179.
[5] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proc. 35th Annu. IEEE Symp. Foundations of Computer Science, 1994, pp. 124–134.
[6] L. Grover, "A fast quantum mechanical algorithm for database search," in Proc. 28th Annu. ACM Symp. Theory of Computing, 1996, pp.212–219.
[7] I. M. Tsai and S. Y. Kuo, "Quantum boolean circuit construction and layout under locality constraint," in Proc. 1st IEEE Conf. Nanotechnology, 2001, pp. 111–116.
[8] J. Cirac and P. Zoller, "Quantum computation with cold trapped ions," Phys. Rev. Lett., vol. 74, pp. 4091–4094, 1995.
[9] Q. Turchette, C. Hood, W. Lange, H. Mabuchi, and H. Kimble, "Measurement of conditional phase shifts for quantum logic," Phys. Rev. Lett., vol. 75, pp. 4710–4713, 1995.
[10] N. Gershenfeld and I. Chuang, "Bulk spin resonance quantum computation," Science, vol. 275, pp. 350–356, 1997.
[11] D. Loss and D. DiVincenzo, "Quantum computation with quantum dots," Phys. Rev. A, vol. 57, pp. 120–126, 1998.
[12] B. Kane, "A silicon-based nuclear spin quantum computer," Nature, vol.393, pp. 133–137, 1998.

八、計畫成果自評

本計畫研究量子電路之合成及檢測的理論，並以實作的方式達成實作 NMR 量子計算系統之雛形，為國內之首例，深具指標意義。本技術不但可用於量子計算系統，亦可用於量子網路上交換系統(量子交換機)之實現，可謂國內一項創舉。

除此之外，目前在本計劃內完成且已被接受之研究論文即達九篇(條列如後)，成果可謂相當豐碩。

(1) I. M. Tsai, S. Y. Kuo, S. L. Huang, Y. C. Lin, and T. T. Chen, "Experimental Realization of an NMR Quantum Switch," Proceedings of the 2004 ERATO conference on Quantum Information Science(EQIS'04), Sept. 2004, Tokyo, Japan.
(2) I. M. Tsai, C. M. Yu, W. T. Tu, and S. Y. Kuo, "A Secure Quantum Communication Protocol using Insecure Public Channels," Proceedings of the 20th International Information Security Conference (SEC'05), May 2005, Chiba, Japan.
(3) I-Ming Tsai and Sy-Yen Kuo, "Performing Authenticated Encryption with Nanoscale Phenomenon", to appear in IEEE-NANO-2005
(4) Han-Wei Wang, I-Ming Tsai and Sy-Yen Kuo, "Protocol and Applications for Sharing Quantum Private Keys", to appear in IEEE-Carnahan-2005
(5) Han-Wei Wang, I-Ming Tsai, Chih-Neng Chung and Sy-Yen Kuo, "A scheme to enhance the error-checking capability of encoded quantum information", to appear in European conference on Circuit theory and design (ECCTD-2005)
(6) C. Y. Lu, S. A. Wang, I. M. Tsai, and S. Y. Kuo, "An Efficient Testing Method for Quantum Boolean Circuits," Proceedings of the 2004 ERATO conference on Quantum Information Science (EQIS'04), Sept. 2004, Tokyo, Japan.

(7) H. W. Wang, I. M. Tsai, and S. Y. Kuo, "A Circuit Approach for Implementing Quantum Memory," Proceedings of the 2004 IEEE Conference on Nanotechnology (IEEE-NANO 2004), August 2004, Munich, Germany.
(8) S. A. Wang, C. Y. Lu, and S. Y. Kuo, "An Efficient Functional Verification Method for Quantum Boolean Circuits," Proceedings of the 2004 IEEE Conference on Nanotechnology (IEEE-NANO 2004), August 2004, Munich, Germany
(9) C. Y. Lu, S. A. Wang, and S. Y. Kuo, "Quantum Boolean Circuits Construction Using Tabulation Method," Proceedings of the 2004 IEEE Conference on Nanotechnology (IEEE-NANO 2004), August 2004, Munich, Germany

可供推廣之研發成果資料表

□ 可申請專利　■ 可技術移轉　日期：94 年 5 月 23 日

國科會補助計畫	計畫名稱：量子計算機之系統架構研究與設計 計畫主持人：郭斯彥 計畫編號：　NSC 93-2218-E-002-098　　學門領域：資訊二
技術/創作名稱	以核磁共振技術實作量子交換機之方法
發明人/創作人	蔡一鳴，郭斯彥
技術說明	中文：目前量子通信網路尚大多由「點對點」之連結所形成。量子通信網路之所以尚未形成真正的「網路」的原因是因為缺乏量子網路上有如傳統交換機或路由器之交換設備。本量子交換技術可使得量子通信網路具有真正的交換功能，大幅化簡目前點對點傳輸之複雜度。 英文：Currently the topology of quantum communication networks is dominated exclusively by the so-called *point-to-point* configuration. The reason why a true *network* is still not popular is that there is no switching or routing capability in the current quantum networks. However, the technology of quantum switching provides a possibility to extend the current quantum *point-to-point* configuration into a true quantum *network*.
可利用之產業及可開發之產品	本技術可供有興趣之廠商將之進一步開發為量子網路上之交換設備(量子交換機)，適合前瞻之資訊，通信等製造業。
技術特點	傳統交換機可傳送古典位元之信號，但無法傳送量子位元之信號。本交換技術可以在達成交換功能之外，並保持原有輸入資訊之量子狀態。此為量子通信網路所必備，但傳統交換設備所無法做到之處。
推廣及運用的價值	本技術推廣及運用的整體價值甚高，因為推廣本技術除可以使廠商在量子通信產業取得領先之優勢外，並可以帶動國內在量子資訊領域之研發及製造風氣，使台灣繼續保持電子資訊製造業大國之地位。

※　1. 每項研發成果請填寫一式二份，一份隨成果報告送繳本會，一份送　貴單位研發成果推廣單位（如技術移轉中心）。

※　**2. 本項研發成果若尚未申請專利，請勿揭露可申請專利之主要內容。**

※　3. 本表若不敷使用，請自行影印使用。