



國立勤益科技大學  
電子工程系研究所碩士班

碩士論文

應用於身體感測網路低功率傳輸接收通道  
編碼晶片設計

**Low-Power Chip Design of Channel Coding for  
Body Area Network Transceiver Systems**

研究生：陳福期

指導教授：林光浩 博士

中華民國 一 百 零 一 年 六 月

應用於身體感測網路低功率傳輸接收通道編碼晶片設計

**Low-Power Chip Design of Channel Coding for Body Area  
Network Transceiver Systems**

研究生：陳福期

指導教授：林光浩 博士

國立勤益科技大學

電子工程系研究所

碩士論文

A Thesis  
Submitted to  
Institute of Industrial Design  
National Chin-Yi University of Technology  
in Partial Fulfillment of the Requirements  
for the Degree of  
Master of Design  
in  
Industrial Design

June 2012

Taiping, Taichung, Taiwan, Republic of China

中華民國 一 百 零 一 年 六 月

# 國家圖書館

## 博碩士論文電子檔案上網授權書

本授權書所授權之論文為授權人在國立勤益科技大學電子工程系  
100 學年度第三學期取得碩士學位之論文。

論文題目：應用於身體感測網路低功率傳輸接收通道編碼晶片設計  
指導教授：林光浩

茲同意將授權人擁有著作權之上列論文全文(含摘要)，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印，此項授權係非專屬、無償授權國家圖書館及本人畢業學校之圖書館，不限地域、時間與次數，以微縮、光碟或數位化方式將上列論文進行重製，並同意公開傳輸數位檔案。

立即開放

上列論文為授權人向經濟部智慧財產局申請專利之附件或相關文件之一（專利申請案號：\_\_\_\_\_），請於 2013 年 07 月 11 日 後再將上列論文公開或上載網路。

因上列論文尚未正式對外發表，請於 2013 年 07 月 11 日 後再將上列論文公開或上載網路。

其他

授權人：陳福期

親筆簽名及蓋章： 陳福期  民國 101 年 7 月 11 日

E-Mail：fire\_ater@yahoo.com.tw

# 國立勤益科技大學

## 博碩士論文全文上網授權書

(提供授權人裝訂於紙本論文書名頁之次頁用)

本授權書所授權之論文為授權人在國立勤益科技大學  
電子工程系 電子工程 組 100 學年度第 二 學期取得碩士學位  
之論文。

論文題目：應用於身體感測網路低功率傳輸接收通道編碼晶片設計  
指導教授：林光浩

### ■ 同意

本人具有著作權之論文全文資料，非專屬、無償授予本人畢業學校圖書館，不限地域、時間與次數，以微縮、光碟或數位化等各種方式重製與利用，提供讀者基於著作權法合理使用範圍內之線上檢索、閱覽、下載及列印。

論文全文上載網路公開之範圍及時間：

校內區域網路	■ 中華民國 102 年 7 月 11 日公開
校外網際網路	■ 中華民國 102 年 7 月 11 日公開

授權人：陳福期

簽名： 陳福期

中華民國 101 年 7 月 11 日

國立勤益科技大學  
研究所碩士班  
論文口試委員會審定書

本校 電子工程系 電子所 碩士班 陳福期 君

所提論文 應用於身體感測網路低功率傳輸接收通道編碼晶片設計

合於碩士資格水準，業經本委員會評審認可。

論文口試委員會：

召集人：

黃瑞州

委員：

黃瑞州

曾振東

林光浩

指導教授：

林光浩

所

長：



中華民國 一 百 零 一 年 六 月

## 摘要

隨著無線通訊技術的蓬勃發展，無線通訊技術已經能應用於人體內外，形成人體區域網路 (Body Area Network, BAN)。由於近年來人口快速老化，如何將無線通訊技術以及醫療技術合併應用於老人健康照護成為未來趨勢。目前以人體周圍的設備，例如隨身攜帶的手錶、感測器、手機以及人體內部 (即植入晶片) 等均可成為無線通信專用系統。而無線網路受限於外在環境的影響，使得傳送訊號會因為訊號耗弱，通訊死角，或是打雷干擾等種種因素造成突發性錯誤 (burst-error)，使得網路無法正常傳輸。本論文提出一個具有突發錯誤更正能力之循環碼快速編解碼硬體改良電路架構，此解碼器適用於有隨機錯誤以及突發錯誤之通道使用。

我們利用 TSMC 0.18 $\mu\text{m}$  設計一個具有 (26,16) 快速編碼之循環碼編碼器以及具突發錯誤更正之循環碼解碼器之晶片。本研究主要包括兩大電路區塊所組成，分別是快速編碼電路和快速解碼電路。晶片共包含 3 萬 7 千個邏輯閘 (gate count)，面積大小為 1.048\*1.048 $\text{mm}^2$ 。本研究對於隨機錯誤之更正能力及突發錯誤之更正能力而言，也都具有相當好的更正能力，解碼器在位元錯誤率為  $10^{-4}$  時，其解碼增益值 (coding gain) 為 2.4dB。

關鍵字：突發性錯誤、循環碼、通道編碼、人體區域網路。

# Abstract

With the rapid development of wireless communication technology, this skill can be applied to body inside and outside, formed body area network (BAN). Due to the population has been aging fast in recent years, wireless communication and medical technology applied to health care for the elderly becomes future trends. The devices of wireless communications system surrounding human body are far-reaching, such as portable watches, sensors, cell phones and microchips [5]. Wireless transmission limited by the interference of the external environment makes the transmitted signal generate burst-error. These factors lead to the data can't be transmitted correctly, such as signal attenuation, communication dead zones and thunder interference. This paper proposes a cyclic code for burst-error correcting capability of fast encoding and decoding hardware improved circuit structure. This decoder is applicable to random error and burst error channel.

To implement above algorithms, we use TSMC 0.18 $\mu$ m 1P6M to design a (26, 16) burst-error-correcting cyclic encoder and decoder chip. This chip is composed of two main circuit blocks. One is a fast encoded cyclic code encoder, and the other is cyclic code decoder of burst-error correction. The proposed chip contains 37K gate counts and occupies the area of 1.048mm by 1.048mm (Including I/O PAD). Additionally, the chip has good correction capacity of the random error correction and burst-error correction. The decoder is in the bit error rate of  $10^{-4}$ , and its coding gain is 2.4dB.

Keywords : burst-error 、 cyclic code 、 channel coding 、 body area network

## 致 謝

七百多天學術研究生活順利結束了，就學期間要感謝許多老師教導、系辦老師的大力相助和同學間互相切磋與幫助。首先誠摯感謝指導教授林光浩博士，在這兩年來細心的教導，方能順利完成本論文，不僅僅在論文上的指導，認真負責的做事態度，更是值得我去效法以及學習的地方。從未接觸生醫系統與數位晶片設計的我，也因老師的帶領漸漸的對晶片設計產生濃厚興趣，在這兩年期間學習不少新知識，並且能夠設計出一顆屬於自己的晶片，。在晶片設計期間，更要感謝國家系統晶片中心提供技術上的支援、教導以及下線機會，讓自己研究成果能夠付諸於實體。

口試期間，感謝交大電信系黃瑞彬教授以及勤益科大曾振東教授在口試時對於本論文提供建議，使本論文能夠更加完善，也多虧了教授們的幫助與指導，讓此次的研究工作畫下的完美的句點。

兩年的研究生活，感謝孟毅學長在上班的閒暇之餘仍然給予我技術上的支援，讓我能夠成功完成研究。高瑞、信有、國轟、聖諺、威盛、東奕、伯軒在研究之餘每個禮拜固定的一起運動打球與嘴砲。阿吉、千華、金爺、禽獸、春雄、眯眯眼、菜頭在各地上班或是同讀研究所的大學同學，常常回來共同聚餐與閒聊。CSIC 實驗室共同奮鬥的學弟妹岱軒、璽諺、威豪、振瑋、源翔、子元、理雄、乙銘、基翎、彥江、堉雅、仁豪、裕鑫。回想起碩士生活的點點滴滴，一同出遊、聚餐，慶生、運動以及研究討論，都讓我的研究生活不乏味並且多采多姿。

最後，僅將本篇論文獻給我摯愛的父母、家人以及默默支持我的小妞，謝謝你們對我的無限包容與疼愛，在遇到挫折與無奈時能夠想起還有你們陪在身旁支持我，讓我能無後顧之憂努力完成想做的事以及碩士學位，希望未來的日子能夠有你們繼續陪伴我，願與你們分享這份喜悅與榮耀。

福期

# 目 錄

摘 要 .....	i
Abstract .....	ii
致 謝 .....	iii
目 錄 .....	iv
圖 目 錄.....	vi
表 目 錄.....	ix
第一章 緒論.....	1
1.1 前言.....	1
1.2 研究背景與動機.....	3
1.3 研究方法.....	4
1.4 章節概要.....	5
第二章 循環碼.....	6
2.1 循環碼簡介.....	6
2.2 縮短循環碼.....	10
2.3 通道錯誤.....	11
第三章 循環碼編碼原理與解碼演算法.....	14
3.1 循環碼編碼原理.....	14
3.1.1 生成多項式.....	14

3.1.2 生成矩陣 .....	16
3.2 循環碼解碼原理 .....	19
3.2.1 查核多項式 .....	20
3.2.2 生成矩陣與查核矩陣 .....	21
3.3 模擬分析 .....	24
3.3.1 錯誤圖樣 .....	24
3.3.2 錯誤更正能力 .....	27
第四章 縮短循環碼硬體編解碼架構 .....	30
4.1 設計流程 .....	30
4.2 縮短循環碼編碼硬體架構 .....	32
4.3 縮短循環碼解碼硬體架構 .....	35
4.4 晶片硬體架構 .....	41
4.5 硬體實現結果 .....	42
第五章 量測結果 .....	47
第六章 結論 .....	53
參考文獻 .....	54
附錄 A. 中英對照表 .....	56

## 圖目錄

圖 1.1 無線通訊系統架構.....	2
圖 1.2 互動式智慧型身體感測網路晶片系統 .....	3
圖 1.3 OFDM 的無線通訊系統 .....	4
圖 2.1 循環碼原理架構 .....	7
圖 2.2 循環碼編碼資料架構.....	9
圖 2.3 二元對稱通道模型圖 .....	11
圖 2.4 加成性白色高斯雜訊通道模型圖 .....	12
圖 2.5 Gilbert-Elliott 突發雜訊通道模組.....	13
圖 3.1 $g(x)$ 的非系統生成矩陣。 .....	17
圖 3.2 $16 \times 26$ 系統生成矩陣。 .....	18
圖 3.3 $(n, k)$ 錯誤檢測與更正示意圖。 .....	19
圖 3.4 $(26,16)$ 縮短循環碼之查核矩陣 .....	23
圖 3.5 徵狀重疊模擬數據.....	26
圖 3.6 縮短循環碼在 AWGN 通道裡的 BER 模擬.....	27
圖 3.7 隨機突發性錯誤(random burst error)示意圖 .....	28
圖 3.8 3-bit burst error 通道裡的 BER 模擬 .....	28
圖 3.9 5-bit burst error 通道裡的 BER 模擬 .....	29
圖 3.10 6-bit burst error 通道裡的 BER 模擬 .....	29

圖 4.1 演算法與硬體實現流程圖 .....	31
圖 4.2 移位暫存器之編碼電路 .....	32
圖 4.3 $16 \times 10$ 係數矩陣。 .....	33
圖 4.4 改良編碼並列式硬體電路架構 .....	34
圖 4.5 移位暫存器之解碼電路 .....	35
圖 4.6 系統查核矩陣的轉置矩陣 .....	36
圖 4.7 改良式徵狀運算並列式硬體電路架構 .....	37
圖 4.8 改良式偵測錯誤並列式硬體電路架構 .....	40
圖 4.9 晶片系統架構圖 .....	41
圖 4.10 編碼器 RTL 模擬結果 .....	43
圖 4.11 解碼器 RTL 模擬結果 .....	43
圖 4.12 編碼器合成後模擬結果 .....	44
圖 4.13 解碼器合成後模擬結果 .....	44
圖 4.14 編碼器佈局後模擬結果 .....	45
圖 4.15 解碼器佈局後模擬結果 .....	45
圖 4.16 晶片佈局設計圖 .....	46
圖 5.1 ADVANTEST V93000 PS1600 自動測試系統 .....	47
圖 5.2 晶片測試數位模組 .....	48
圖 5.3 編碼資料完整性 .....	49

圖 5.4 解碼資料完整性..... 49

圖 5.5 電壓-頻率比較圖 ..... 50

圖 5.6 晶片佈局設計圖..... 50



# 表 目 錄

表 1.1 人體生理資訊之訊號特性表 .....	1
表 3.1 錯誤位元與徵狀比對表 .....	24
表 4.1 錯誤圖樣偵錯電路演算法 .....	39
表 4.2 晶片預期規格表 .....	46
表 5.1 晶片實測規格表 .....	51
表 5.2 本論文與參考文獻晶片效能比較 .....	52



# 第一章 緒論

## 1.1 前言

近年來人口快速老化，如何將無線通訊技術以及醫療技術合併應用於老人健康照護成為未來趨勢，人類的一些重要的基本生理資訊，例如：血壓值、心電圖、腦波圖、血壓、血氧等如表 1.1 所示。目前市面上可見到的健康監護設備以植入人體或是黏貼在人體表面為主，如穿戴於指尖的血氧傳感器、腕錶型血糖傳感器、腕錶型睡眠品質測量器、睡眠生理檢查器、可植入型身份識別組件等，皆是無線通訊來進行資料的傳輸[1]-[3]。有了人體區域網路( Body Area Network, BAN)，這些感測器和無線網路則都能共同工作，並配置相同的通信元件，使通信資源能夠更有效的利用[4], [5]。

表 1.1 人體生理資訊之訊號特性表

生理訊號	量測參數	訊號頻寬 (Hz)	Sampling Rate (Hz)	A/D resolution	量測方法
心電圖(ECG)	0.5~4mV	DC~50	300	8 bits	Skin electrodes
肌電圖(EMG)	0.1~5mV	DC~10000	1000	8 bits	Needle electrodes
腦波圖(EEG)	5~300uV	DC~150	300	8 bits	Scalp electrodes
血壓(BP)	5~400mmHg	DC~50	200	8 bits	Pressure gage
血氧(SpO <sub>2</sub> )	比例式取得	0.1~0.33	125	8 bits	紅外線

人體網路的功率消耗和元件大小是人體通訊設備設計中最重要之事項，也是最需要克服的問題，雖然現代積體電路技術已相當成熟，但是在植入性的醫療電子裝置應用上，低功率的需求還是具有相當大的挑戰性。一般資料在通道(channel)的傳輸過程中，會受到外在環境的雜訊干擾，使得原本傳輸的資料摻雜了錯誤序列在其中。因此在無線網路裡，良好的錯誤更正碼可以有效地應用在資料傳輸過程中，以降低資料的錯誤率。

圖 1.1 為一個典型的無線通訊系統架構圖，在傳輸端包含了資料源(source data)、錯誤更正編碼器(error correction encoder)、調變器(modulator)；接收端包含了解調變器(demodulator)、錯誤更正解碼器(error correction decoder)、接收資料(receiver data)，其中錯誤更正編碼器與錯誤更正解碼器通稱為 channel coding。在一般數位通信系統的簡化模型中，發送端的信號源產生二進位碼的資料，再由通道編碼器依照預定的規則加入冗餘(Redundancy)位元，之後將其送到通道中，經過通道中雜訊的干擾後，到達接收端經由通道解碼器將冗餘位元移除，並判斷所傳送的資料是否正確，這便是數位通訊的基本架構。本文的重點即在其中的通道編碼器 (Channel Encoder) 與通道解碼器 (Channel Decoder)，如圖 1.1 紅色虛框所示。

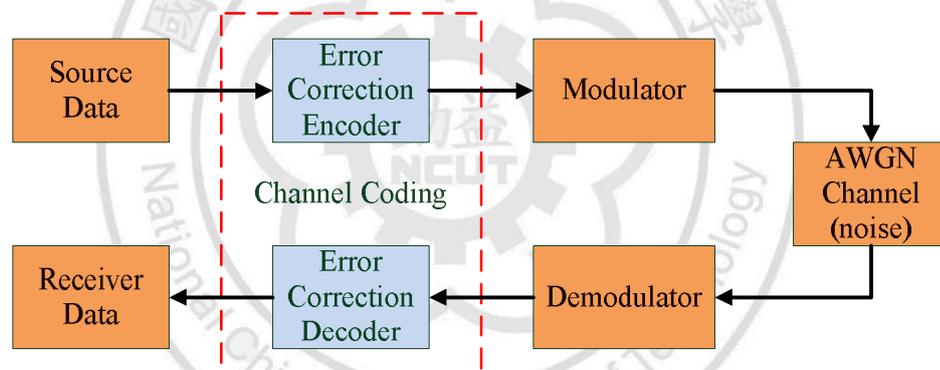


圖 1.1 無線通訊系統架構

本文專注的主軸為無線通訊系統中的通道編解碼，無線資料傳輸之功率和效能是最主要克服的問題，並且使用數位訊號處理設計方案來降低功率消耗，改良傳統的循環碼硬體架構，使其能增加資料的吞吐量(throughput)與增進系統效能之可靠度，在面對突發性錯誤或隨機性錯誤，都具有一定的錯誤更正能力。

## 1.2 研究背景與動機

人體外部許許多多的生理訊號，皆可以透過相關的電子感測裝置直接或間接取得(如：心跳、血壓與體溫等)，而個人的生理健康狀況也可以從而得知。但市面上的醫療器材卻是各自獨立，若是經由醫師囑咐特定時間去量測與監控，對於行動不便或是失智的病患，將造成相當大的困擾，除了忘記正確的紀錄病理資料外，更可能因沒有定時的監控生理參數而造成健康及生命的威脅。為了兼顧使用上的便利性，讓使用者可以在一般日常坐息，甚至移動時，皆可以隨時監控到自身的生理狀況，因此無線穿戴式全身生理訊號檢測系統便成為近年來各生物醫學、網路與電子相關領域研究的熱門課題。

圖 1.2 是互動式智慧型身體感測網路晶片系統 (Interactive Intelligent Body Area Network SOC) 構想[6]，其中包含了低功率生理訊號無線傳輸接收系統晶片、低功率智慧型通訊網路、低功率類比數位介面系統晶片、嵌入式電源管理與訊號處理軟體系統開發、低功率無線傳輸接收基頻系統晶片等，之間的訊息傳輸皆需透過無線傳輸技術。

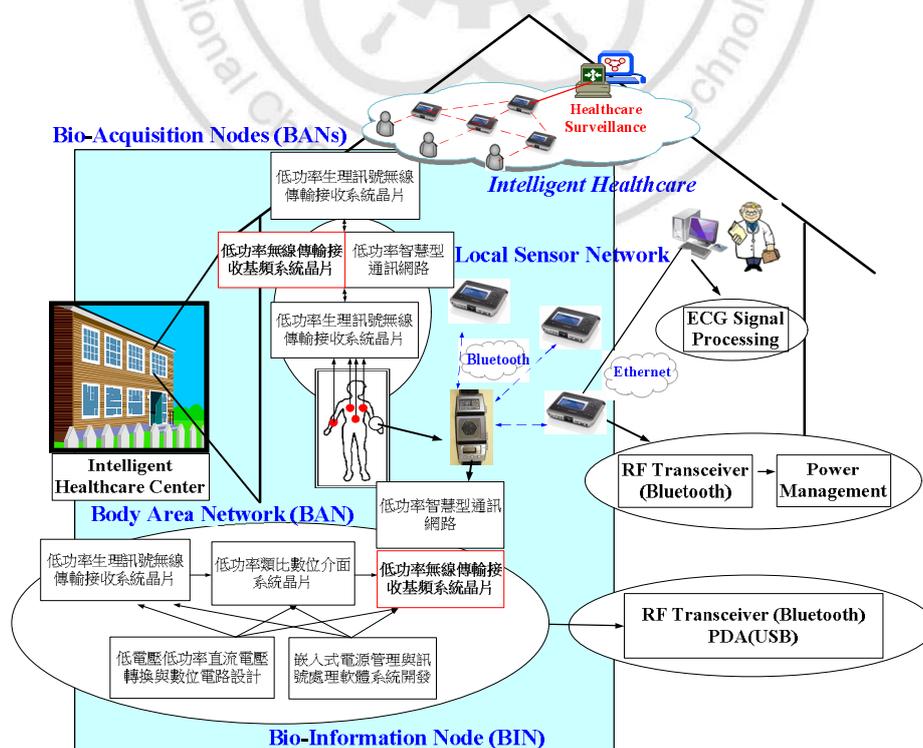


圖 1.2 互動式智慧型身體感測網路晶片系統

低功率無線傳輸的技術上有藍芽(Bluetooth)、正交分頻多工(Orthogonal frequency-division multiplexing, OFDM)和無線感測網路(ZigBee)等技術[4]，藍芽傳輸速率較低可做為語音與資料傳輸，OFDM 具備高速率資料傳輸的能力，加上能有效對抗頻率選擇性衰減，而逐漸獲得重視與採用。ZigBee 是一種低價位、低耗電量的短距離無線通訊技術，主要用於連接家庭內的電器控制。因此為了使無線傳輸能有較佳的信號可靠度，所以使用通道編碼來增加信號的可靠度，並且應用於低功率無線傳輸接收基頻系統晶片裡。

### 1.3 研究方法

本研究所採用的通道編碼為循環碼(Cyclic Code)，它的優點是容易編碼且具有嚴謹的數學架構，其性能容易去分析。循環碼本身具有循環特性，對於編碼的電路簡單易於實現。主要應用於 OFDM 的無線通訊系統上，如圖 1.3 所示。傳輸資料由 MAC 送出資料源(Data stream)經由向前錯誤控制源編碼器(Forward Error Control, FEC)編碼，接著交錯碼與映射(Interleaving and Mapping)把資料轉換成複數資料，然後利用反快速傅立葉轉換(Inverse Fast Fourier Transform, IFFT)，將複數資料調變至不同的子載波上，並加上保護區間(Guard Interval, GI)以有效克服符元間的干擾，在訊號傳送前還需經過數位轉類比轉換器(Digital-to-Analog Converter, DAC)與濾波器(Filter)轉換成類比資料，最後經由 IQ 調變與高功率放大器(HPA)調整到系統規範的頻段進行傳輸，在接收端分別是相當於傳送端各部分功能進行反向操作，以便進行訊號解調還原資料。

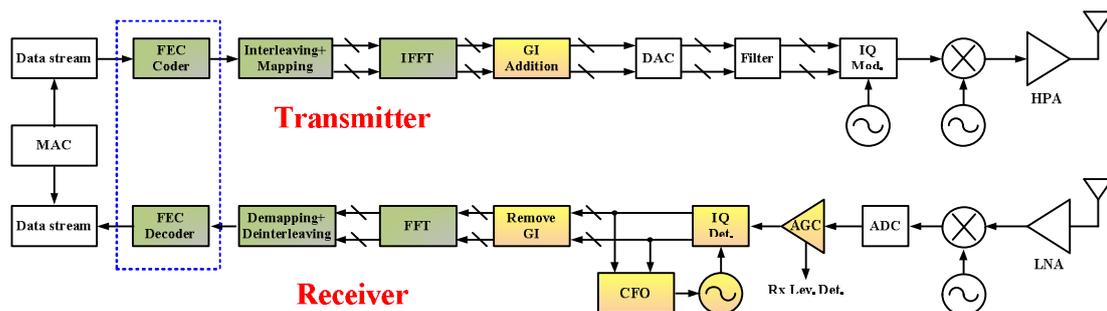


圖 1.3 OFDM 的無線通訊系統

從基本的循環碼演算法搭配軟體 Matlab 開始進行模擬，藉由模擬中找尋新的硬體架構，之後分析並比較現有的演算法，以找出最適合使用的演算法，最後在不損失位元錯誤率(Bit Error Rate, BER)效能下，以硬體面積與複雜度為考量修改演算法，並且利用 Synopsys 軟體去實現改良式硬體。

## 1.4 章節概要

本論文總共分為六個章節，其內容綱要如下：

### 第一章緒論

介紹本論文之研究背景、動機及方法、並且對論文架構和應用方向作一簡略的介紹。

### 第二章循環碼

描述循環碼的歷史與基本概念，同時也介紹縮短循環碼以及循環冗餘碼的應用。

### 第三章循環碼編碼原理與解碼演算法

介紹循環碼編碼原理與解碼演算法，並且針對突發性錯誤(burst error)去做系統的通道模擬。

### 第四章 CRC 硬體編解碼架構

針對本論文所提出之 CRC 架構進行改良與硬體實現，將資料傳輸模式由串列改良成並列，增加資料的吞吐量。

### 第五章結論

對於本論文之研究成果作出結論，並提出未來改進之方向。

## 第二章 循環碼

本章節首先介紹循環碼的基本概念以及原理定義，接著細項探討縮短循環碼的實際應用與通道錯誤的影響。

### 2.1 循環碼簡介

1948 年香農(Shannon)在他的開創性論文“通訊的數學理論”中，首次闡明了在有擾通道中實現可靠通訊的方法，提出了著名的有擾通道編碼定理，奠定了糾錯碼的基礎[7]。自此以後漢明(Hamming)、斯列賓(Slepian)、普蘭奇(Prange)等人在 50 年代初，根據香農的思想，設計出一系列有效的編碼與解碼方法。以後，糾錯碼受到了越來越多的通訊與數學工作者，特別是代數學家的重視，使糾錯碼無論在理論還是在實際中都得到快速的發展[8]。

循環碼(cyclic codes)為線性碼中一個相當重要的類別，是由 Prange 第一次發表於[9]。在此之後，循環碼被代數學家並有很豐富的研究結果[10]-[13]。近代有些特殊的循環碼(如 BCH 碼及 Reed-Solomon 碼)更被用於太空通訊、衛星通訊、光碟儲存、視訊廣播等等系統。被廣泛應用的原因有兩點：一是循環碼具有嚴謹的代數結構，其性能易於分析，特別是目前已發現的大部分線性碼，皆與循環碼有密切的關係，他們之中大部分的碼都可歸結於循環碼；二是循環碼具有循環特性，可以簡單的利用迴授移位暫存器去完成電路架構，特別是編碼電路簡單易於實現。

循環碼是對每段  $k$  位元長的訊息組，以一定規則增加  $n-k$  個校驗位元，組成長度為  $n$  的序列： $(c_{n-1}, c_{n-2}, \dots, c_1, c_0)$ ，稱這個序列為碼字(code word)。在二進制情況下，訊息位元組總共有  $n$  個位元，因此通過編碼器後，相應的碼字也有  $2^k$  個，稱這  $2^k$  個碼字集合為  $(n, k)$  碼。

如圖 2.1 之範例，在傳送端編碼的部分，資料( $a_3 \sim a_0$ )會先經由一個生成多項式(generator polynomial)去做除法運算，而產生的餘數，即是三位元的檢查位元( $r_2 \sim r_0$ )；在接收端解碼時，所收到的 7 位元資料源，會經由徵狀(syndrome)電路去算出徵狀( $s_2 \sim s_0$ )，如果徵狀等於零，則代表資料正確無誤，可以直接輸出所接收到的資料；若徵狀不為零的話，則代表資料有錯誤。

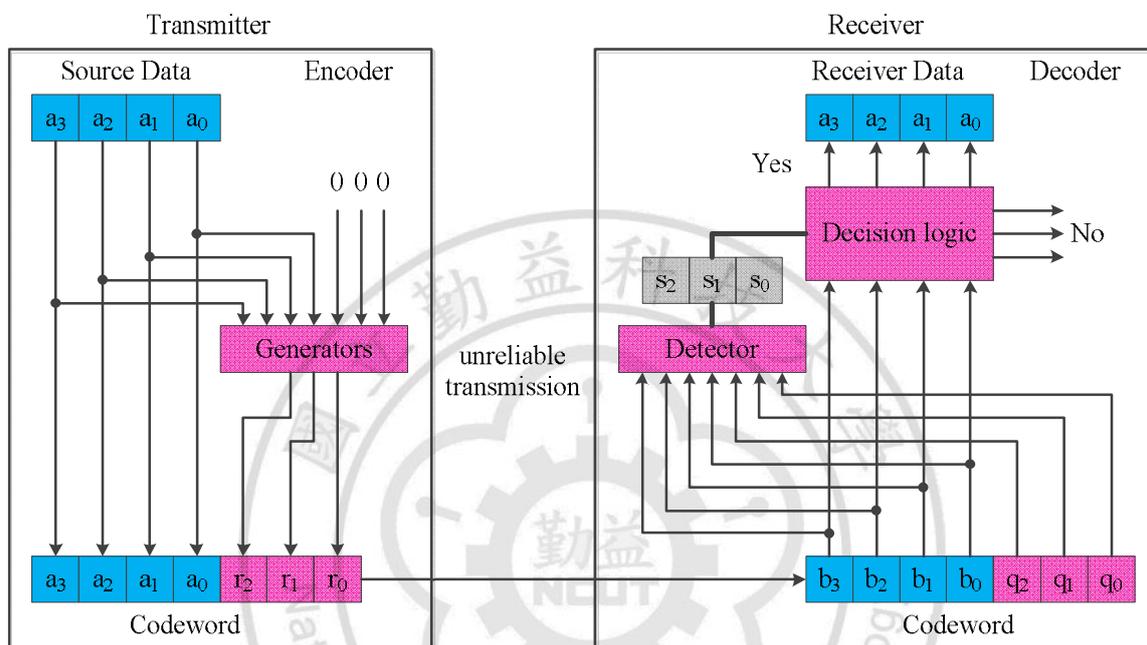


圖 2.1 循環碼原理架構

循環碼的編碼方式有兩種：一種是透過多項式進行編碼，另外是利用同位查核(Parity check)多項式進行編碼。有關循環碼之解碼，先推導循環碼的徵狀，再利用偵錯邏輯閘去進行修改錯誤，而徵狀計算可以利用移位暫存器來完成。

循環碼的基本性質是任意兩編碼字移位的結果亦為編碼字，此性質可以用數學描述，若 $(C_0, C_1, \dots, C_{n-1})$ 為編碼字，其結構為 $(n, k)$ 線性碼，因為它為循環碼所以 $(C_{n-1}, C_0, \dots, C_{n-2})$ ， $(C_{n-2}, C_{n-1}, \dots, C_{n-3})$ ， $\dots$ ， $(C_1, C_2, \dots, C_{n-1}, C_0)$ 均為編碼字。

要發展循環碼的代數關係可以用  $(C_0, C_1, \dots, C_{n-1})$  為係數定義編碼多項式 (code polynomial)，如下

$$c(X) = c_0 + c_1X + c_2X^2 + \dots + c_{n-1}X^{n-1} \quad (2.1)$$

$X$  為未知數。因為我們所討論的為二進位，所有係數非 0 即 1，每個  $X$  的乘冪代表上一位元的移位，也就是在多項式  $c(X)$  乘以  $X$  表示向右移一位。若編碼多項式為  $c(X)$ ，乘以  $X^i$  得到

$$\begin{aligned} X^i c(X) &= X^i (c_0 + c_1X + \dots + c_{n-i-1}X^{n-i-1} + c_{n-i}X^{n-i} + \dots + c_{n-1}X^{n-1}) \\ &= c_0X^i + c_1X^{i+1} + \dots + c_{n-i-1}X^{n-1} + c_{n-i}X^n + \dots + c_{n-1}X^{n+i-1} \\ &= c_{n-i}X^n + \dots + c_{n-1}X^{n+i-1} + c_0X^i + c_1X^{i+1} + \dots + c_{n-i-1}X^{n-1} \end{aligned} \quad (2.2)$$

在最後一行重新調整次序，所以在(2.2)式的前  $i$  次項為

$$\begin{aligned} X^i c(X) &= c_{n-i} + \dots + c_{n-1}X^{i-1} + c_0X^i + c_1X^{i+1} + \dots + c_{n-i-1}X^{n-1} + c_{n-i}(X^n + 1) \\ &+ \dots + c_{n-1}X^{i-1}(X^n + 1) \end{aligned} \quad (2.3)$$

定義

$$c^{(i)}(X) = c_{n-i} + \dots + c_{n-1}X^{i-1} + c_0X^i + c_1X^{i+1} + \dots + c_{n-i-1}X^{n-1} \quad (2.4)$$

$$q(X) = c_{n-i} + c_{n-i+1}X + \dots + c_{n-1}X^{i-1} \quad (2.5)$$

依(2.3)式可將多項式簡寫成

$$X^i c(X) = q(X)(X^n + 1) + c^{(i)}(X) \quad (2.6)$$

$c^{(i)}(X)$  為碼字  $(C_{n-i}, \dots, C_{n-1}, C_0, C_1, \dots, C_{n-i-1})$  所組成的編碼多項式。由(2.6)式亦知  $c^{(i)}(X)$  為  $X^i c(X)$  除以  $(X^n + 1)$  的餘數，因此我們正式的以多項式表示說明它的循環特性。若  $c(X)$  為一編碼多項式，則

$$c^{(i)}(X) = X^i c(X) \bmod (X^n + 1) \quad (2.7)$$

亦為循環移位  $i$  後的編碼多項式。

循環碼擁有線性 (linear) 性質，由任意兩編碼字以 2 為基底運算的結果亦為碼字。考慮一個 (n, k) 循環段碼，其中 k 位元與傳送信號內容相同，其餘的 n-k 位元則依預設的規則計算出來，這些 n-k 位元稱為廣泛性查核位元 (generalized parity check bits) 或簡稱查核位元 (parity bits)。在碼字中訊息位元在傳送時沒有改變，因此也稱為系統碼 (systematic code)。

令  $m_0, m_1, \dots, m_{k-1}$  組成一 k 位元的訊息段，這樣子我們有  $2^k$  種不同的訊息段，將這訊息段輸入編碼器，輸出 n 個位元的編碼字以  $c_0, c_1, \dots, c_{n-1}$  表示。令  $b_0, b_1, \dots, b_{n-k-1}$  表示 (n-k) 個查核位元。對於有系統架構的碼，其編碼字分為兩部份其一代表訊息位元，另一部份則為查核位元，如圖 2.2 所示，k 個最左端的為訊息位元，而 (n-k) 個最右端的位元為查核位元。我們可以寫成

$$c_i = \begin{cases} b_i, & i = 0, 1, \dots, n-k-1 \\ m_{i+k-n}, & i = n-k, n-k+1, \dots, n-1 \end{cases} \quad (2.8)$$

(n-k) 個查核位元為 k 個訊息位元的線性合 (linear sums) 如下所示

$$b_i = p_{0i} m_0 + p_{1i} m_1 + \dots + p_{k-1i} m_{k-1} \quad (2.9)$$

係數的定義如(2.10)，係數  $P_{ij}$  的選擇是使生成矩陣 (generator matrix) 的各列為線性獨立，並且查核式為唯一。

$$P_{ij} = \begin{cases} 1, & \text{if } b_i \text{ depends on } m_j \\ 0, & \text{otherwise} \end{cases} \quad (2.10)$$

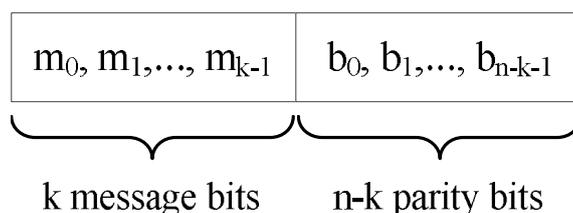


圖 2.2 循環碼編碼資料架構

## 2.2 縮短循環碼

循環碼生成多項式必是  $x^n - 1$  的因式，但在絕大部分  $n, k$  中的  $x^n - 1$  的因式相對而言比較少，限制了碼字的個數。為了增加  $n, k$  取值的數目增加碼字個數，循環碼經常用縮短形式，得到縮短循環碼。

縮短循環碼是取  $[n, k]$  循環碼中前  $i$  為訊息為 0 的碼字作為碼字，構成一個  $(k - i)$  維線性子空間，得到一個  $[n - i, k - i]$  ( $1 \leq i \leq k$ ) 縮短循環碼。縮短循環碼的校驗位元仍為  $n - k$ ，故該碼的糾錯能力至少不低於原來的  $[n, k]$  碼，並且他的實現也並不比循環碼複雜。

縮短循環碼的生成多項式與原本的循環碼相同，均為  $g(x)$ ，故編碼電路與原碼相同。縮短循環碼的  $G$  矩陣可以從循環碼的標準  $G$  陣中去掉前  $i$  行和前  $i$  列得到， $H$  矩陣可以從原典型的  $H$  陣中去掉前  $i$  列得到。

如果要由  $[7, 4]$  循環碼縮短一位元，便得到了  $[6, 3]$  縮短碼，他的  $G$  和  $H$  矩陣可直接由  $[7, 4]$  碼得到。

$$\mathbf{G}_{[7,4]} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \Rightarrow \mathbf{G}_{[6,3]} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$\mathbf{H}_{[7,3]} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \Rightarrow \mathbf{H}_{[6,3]} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

由上述  $\mathbf{G}_{[6,3]}$  矩陣可以明顯看到，縮短循環碼的碼字間不一定存在有循環關係。但是這並不會影響解碼器的複雜性，以後將看到縮短循環碼的解碼器僅在原碼解碼器基礎上，稍加做修改即可。

## 2.3 通道錯誤

在實際的通訊系統中，所傳送的資料會因為傳輸時所經過通訊頻道性質的不同，而受到不同形式的干擾，使得資料在傳輸過程中發生錯誤。在有線環境中，由於通道狀態較穩定，所以傳輸的資料發生錯誤的機率不高；但是在無線環境中，由於一些空氣介面的特性及多路徑衰減(multipath fading)、陰影效應(shadowing)和頻道干擾(channel interference)等現象，使得傳輸資料的錯誤率大幅提高，而且錯誤的發生亦呈現時變性(time-varying)和叢發性(bursty)。

本文探討的通道模型為二元對稱通道、加成性白色高斯雜訊通道和 Gilbert-Elliott 圖雜訊通道模組。如圖 2.3 為二元對稱通道模型圖，其中  $1-p$  和  $p$  分別代表傳送無錯誤機率與傳送失真機率。對於傳送無錯誤機率  $1-p$ ，是指傳送訊息與接收訊息為相同的機率，即為

$$P(r = 1|c = 1) = P(r = 0|p = 0) = 1 - p \quad (2.11)$$

至於傳送失真機率  $p$ ，則可表示為

$$P(r = 1|c = 0) = P(r = 0|p = 1) = p \quad (2.12)$$

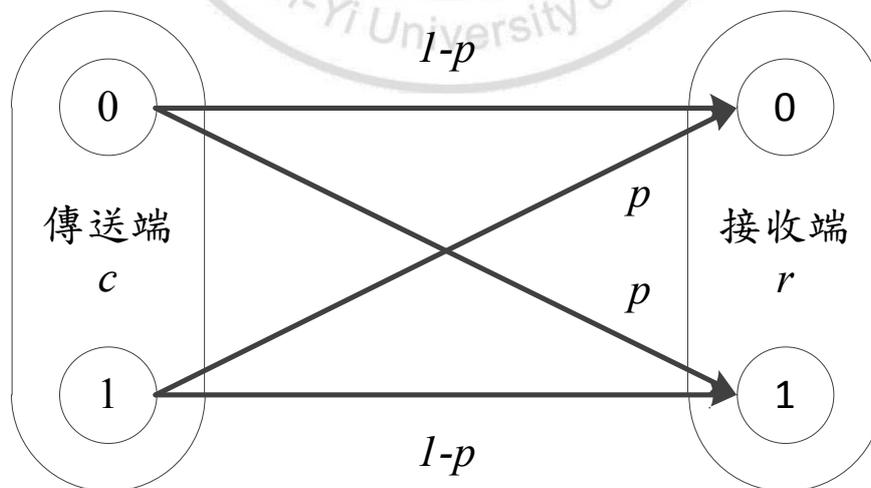


圖 2.3 二元對稱通道模型圖

圖 2.4 為加成性白色高斯雜訊(Additive White Gaussian Noise, AWGN)通道模型圖。加成性白色高斯雜訊通道的通道機率可表示如(2.13)方程式。

$$P(r_i|c_i) = \frac{1}{\sqrt{\pi N_0}} e^{-\frac{(r_i-c_i)^2}{N_0}} \quad (2.13)$$

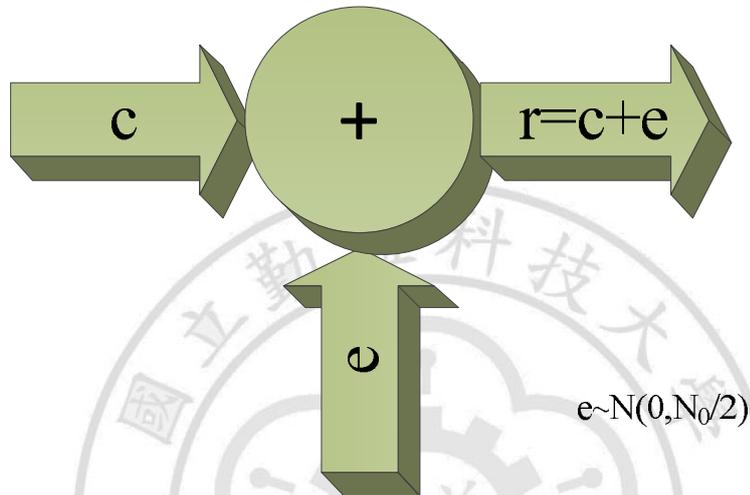


圖 2.4 加成性白色高斯雜訊通道模型圖

其中  $N_0$  為單邊雜訊功率頻譜密度(power spectral density)。對於此通道的通道容量部分，Shannon 證明該通道的通道容量  $C$  可表示如下[7]:

$$C = W \log_2 \left( 1 + \frac{P}{N_0 W} \right) = W \log_2 \left( 1 + \frac{E_b R}{N_0 W} \right) \quad (2.14)$$

其中  $\frac{E_b}{N_0}$  為位元雜訊能量比(bit energy to noise spectral density ratio)、 $P$  為輸入功率、 $R$  為碼率(code rate)，以及  $W$  為通道頻寬。

Gilbert-Elliott 突發雜訊通道模組 (Burst Noise Channel Model) 是由 Gilbert[20]-[23]所提出，此模組綜合了許多其他的突發雜訊通道之特性，並且實際模擬通道中之可能因素所形成之模組。此模組是由兩個狀態的馬可夫鏈 (Markov Chain) 所組成，如圖 2.5 所示。

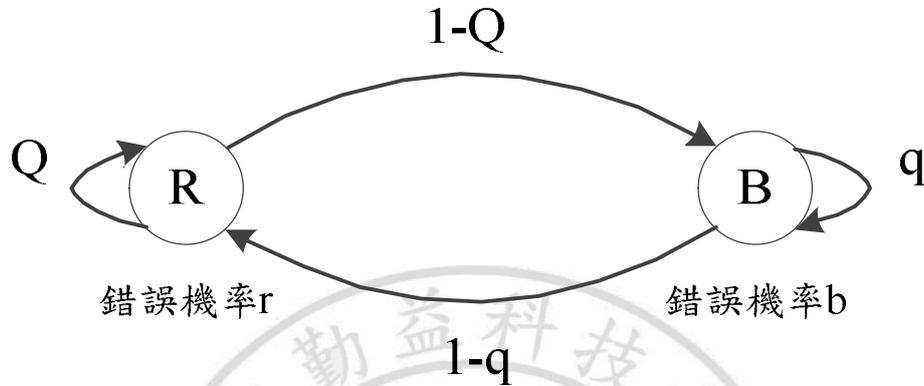


圖 2.5 Gilbert-Elliott 突發雜訊通道模組

圖 2.5 中的狀態 R 為隨機錯誤狀態(Random error state)，而 B 為突發錯誤狀態(Burst error state)；位元訊息在狀態 R 時發生位元錯誤的機率為 r，在狀態 B 所發生的位元錯誤機率為 b。並且給定兩個條件機率值為 Q 和 q。有了上述條件設定，我們便可以利用矩陣的方式來表是機率轉移  $\mathbf{P}$ ，如式(2.15)

$$\mathbf{P} = \begin{bmatrix} Q & 1-Q \\ 1-q & q \end{bmatrix} \quad (2.15)$$

為了表示平均位元錯誤率  $P_e$ ，我們定義狀態 B 的位元錯誤率為  $P_B$ ，狀態 R 的位元錯誤率為  $P_R$ ，便可得到式(2.16)

$$\begin{aligned} P_B &= \frac{1-Q}{2-Q-q} \\ P_R &= \frac{1-q}{2-Q-q} \end{aligned} \quad (2.16)$$

再利用式(2.16)便可以得到平均位元錯誤率  $P_e = b \times P_B + r \times P_R$ 。若假設位元錯誤的機率高於平均為元錯誤  $P_e$  時，就會產生所謂的突發錯誤。

## 第三章 循環碼編碼原理與解碼演算法

本章節將詳細的介紹循環碼編碼和解碼的演算法，針對生成方程式與矩陣這兩種表示方法去做解說，以及徵狀的計算與比對錯誤原理。

### 3.1 循環碼編碼原理

#### 3.1.1 生成多項式

依據(2.6)與(2.7)即可證明多項式  $X^n + 1$  及其因式在產生循環碼的過程有重要關鍵。令  $g(X)$  為  $n-k$  階以  $X^n + 1$  為因式的多項式，它是編碼裡最低冪數的多項式，一般  $g(X)$  可寫成

$$g(X) = 1 + \sum_{i=1}^{n-k-1} g_i X^i + X^{n-k} \quad (3.1)$$

係數  $g_i$  為 0 或 1。依據這種展開式，多項式  $g(X)$  有兩項的係數為 1，其間分隔  $n - k - 1$  項。多項式  $g(X)$  稱為循環碼的生成多項式。一個循環碼可由其生成多項式唯一決定，其編碼多項式可表示如(3.2)式。 $a(X)$  為  $X$  的  $k - 1$  次冪， $c(X)$  也滿足(2.7)式，因為  $g(X)$  是  $X^n + 1$  的因式。

$$\begin{aligned} a(X) &= X^{k-1} \\ c(X) &= a(X)g(X) \end{aligned} \quad (3.2)$$

假設令訊息多項式為  $m(X) = m_0 + m_1X + \dots + m_{k-1}X^{k-1}$ ，而查核多項式為

$b(X) = b_0 + b_1X + \dots + b_{n-k-1}X^{n-k-1}$  依據循環碼形式，我們希望編碼多項式有下列的型式

$$c(X) = b(X) + X^{n-k}m(X) \quad (3.3)$$

運用(3.2)式及(3.3)式可得  $a(X)g(X) = b(X) + X^{n-k}m(X)$  也可寫成(3.4)並

說明了多項式  $b(X)$  是  $X^{n-k}m(X)$  除以  $g(X)$  後的餘數。

$$\frac{X^{n-k}m(X)}{g(X)} = a(X) + \frac{b(X)}{g(X)} \quad (3.4)$$

彙整上述的說明，對於編製一個(n,k)循環碼具有系統結構的步驟如下：

1. 首先將訊息多項  $m(X)$  乘以  $X^{n-k}$ 。
2. 將  $X^{n-k}m(X)$  除以  $g(X)$  得到  $b(X)$ 。
3. 將  $b(X)$  加入  $X^{n-k}m(X)$  得到編碼多項式。

本研究主要是使用擁有最理想的突發性錯誤修正 (burst-error-correcting) 縮短循環碼 (shortened cyclic code)，而他原始代碼是 341 位元的自然循環長度縮短了 325 位元，形成了現在的 26 位元碼字，下列式經由縮短之後的生成多項式：

$$g(x) = x^{10} + x^8 + x^7 + x^5 + x^4 + x^3 + 1$$

這 10 位元基礎縮短循環碼之偵錯位元以普遍的方式形成，換言之，它是被  $x^{n-k}$  乘法運算後所剩的餘數項，而且它們被分配到生成多項式  $g(x)$ ，根據(3.4)的表示方式，這基本碼向量  $v(x)$  可表示成：

$$v(x) = m(x)x^{10} + \frac{m(x)x^{10}}{g(x)} \bmod g(x)$$

首先，向量碼從最高位元開始傳送。例如：傳送資料位元  $c_{25}x^{25}$  to  $c_{10}x^{10}$ ，接著傳送修正偵測位元  $c_9x^9$  to  $c_0x^0$ 。

### 3.1.2 生成矩陣

(2.8)式與(2.9)式說明  $(n, k)$  線性段碼的數學結構，這些方程式可用矩陣表示法更簡潔的說明。為了使得推導順我們定義  $1 \times k$  訊息向量  $\mathbf{m}$ ，

$1 \times (n - k)$  查核向量  $\mathbf{b}$  與  $1 \times n$  編碼向量  $\mathbf{c}$  如下

$$\mathbf{m} = [m_0, m_1, \dots, m_{k-1}] \quad (3.5)$$

$$\mathbf{b} = [b_0, b_1, \dots, b_{n-k-1}] \quad (3.6)$$

$$\mathbf{c} = [c_0, c_1, \dots, c_{n-1}] \quad (3.7)$$

這些向量皆為列向量 (row vectors)，在編碼領域裡經常以列向量為主要表示。由於查核位元為訊息位元的線性合，用矩陣可以表示如(3.8)式

$$\mathbf{b} = \mathbf{mP} \quad (3.8)$$

$\mathbf{P}$  為  $k \times (n - k)$  係數矩陣，定義如下 ( $P_{ij}$  為 0 或 1)：

$$\mathbf{P} = \begin{bmatrix} P_{0,0} & \cdots & P_{0,n-k-1} \\ \vdots & \ddots & \vdots \\ P_{k-1,0} & \cdots & P_{k-1,n-k-1} \end{bmatrix} \quad (3.9)$$

由(3.5)至(3.7)式的定義，向量  $\mathbf{c}$  可以表示成

$$\mathbf{c} = [\mathbf{m}|\mathbf{b}] \quad (3.10)$$

因此將(3.8)式代入(3.10)式，並提出共通項次(訊息向量)成為

$$\mathbf{c} = \mathbf{m}[\mathbf{I}_k|\mathbf{P}] \quad (3.11)$$

$\mathbf{I}_k$  代表  $k \times k$  單位矩陣 (identity matrix)：

$$\mathbf{I}_k = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \quad (3.12)$$

定義  $k \times n$  生成矩陣 (generators matrix) 為

$$\mathbf{G} = [\mathbf{I}_k | \mathbf{P}] \quad (3.13)$$

生成矩陣  $\mathbf{G}$  稱為正規梯陣 (echelon canonical form)，其  $k$  列向量均為線性獨立，亦即  $\mathbf{G}$  矩陣內的任意列向量均不能由其他列向量表示。利用生成矩陣  $\mathbf{G}$  的定義，可以簡化(3.10)式如(3.14)式所示

$$\mathbf{c} = \mathbf{mG} \quad (3.14)$$

依照生成方程式所取得的  $1 \times 16$  向量  $[10110111001]$ ，並且在後面補上  $k - 1$  個零，之後再一一的移位產生  $16 \times 26$  的生成矩陣，由圖 3.1 之中可以看出此矩陣並非系統式格式。藉由式(3.9)，計算出  $16 \times 10$  的係數矩陣  $\mathbf{P}$ ，再利用式(3.12)，加上  $16 \times 16$  的單位矩陣，即可得到如圖 3.2  $16 \times 26$  的系統生成矩陣了。

$$\mathbf{G}_1 = \begin{bmatrix} 10110111001000000000000000 \\ 01011011100100000000000000 \\ 00101101110010000000000000 \\ 00010110111001000000000000 \\ 00001011011100100000000000 \\ 00000101101110010000000000 \\ 00000010110111001000000000 \\ 00000001011011100100000000 \\ 00000000101101110010000000 \\ 00000000010110111001000000 \\ 00000000001011011100100000 \\ 00000000000101101110010000 \\ 00000000000010110111001000 \\ 00000000000001011011100100 \\ 00000000000000101101110010 \\ 00000000000000010110111001 \end{bmatrix}$$

圖 3.1  $g(x)$  的非系統生成矩陣。



### 3.2 循環碼解碼原理

上述所講的生成矩陣  $G$  是的使用在發射端之編碼運算，而這章節的查核矩陣  $H$  則是在接收端的解碼運算。當接收端接收到  $r$  為  $1 \times n$  的接收向量時，它是編碼向量  $c$  通過有雜訊通道的結果。我們可以用下式表示

$$r=c+e \quad (3.15)$$

向量  $e$  稱為誤差向量或誤差圖樣 (error pattern)。誤差向量  $e$  的第  $i$  元素若為 0 則表示第  $i$  元素的  $r$  向量與  $c$  向量相同，若誤差向量  $e$  的第  $i$  元素為 1，則表示第  $i$  元素的  $r$  向量與  $c$  向量不同，其中  $i=1,2,\dots,n$ ，所以

$$e_i = \begin{cases} 1, & \text{If an error has occurred in the } i^{\text{th}} \text{ location} \\ 0, & \text{otherwise} \end{cases} \quad (3.16)$$

接收端必須有一個檢查機制將接收向量  $r$  解調為編碼向量  $c$ 。一般通道的解碼程序是利用查核矩陣  $H$  去運算出錯誤徵狀向量 (error-syndrome vector) 或簡稱徵狀，並且與誤差圖樣進行比對更正。給定接收向量  $r$ ，相對的徵狀為

$$s = rH^T \quad (3.17)$$

如圖 3.3 所示，接收到了  $n$  位元的字碼，經由查核矩陣進行徵狀的運算，如果徵狀等於零，則表示傳送的  $n$  位元資料無誤；若不等於零，則代表資料有錯誤，因此資料需要進一步執行錯誤更正。藉由比對徵狀字元，去判別錯誤位元是第幾位元，之後再經由偵測器去做資料更正。

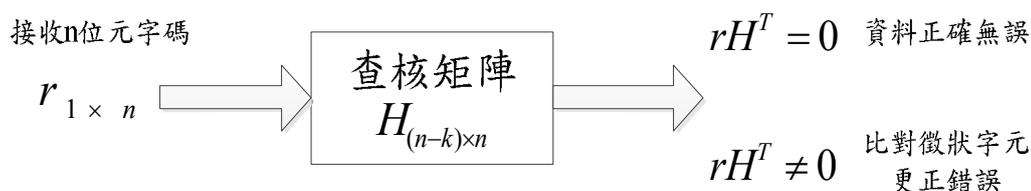


圖 3.3  $(n, k)$  錯誤檢測與更正示意圖。

### 3.2.1 查核多項式

一個(n,k)循環碼是由(n-k)幕次的生成多項式唯一決定的。不過它也可由另一 k 幕次的查核多項式唯一決定。查核多項式定義如下：

$$h(x) = 1 + \sum_{i=1}^{k-1} h_i X^i + x^k \quad (3.18)$$

$h_i$  的係數為 0 或 1。查核多項式  $h(X)$  也有與生成多項式類似的型式，它有兩項的係數為 1，其間的時間為  $k-1$  項。產生多項式  $g(X)$  等效於生成矩陣  $G$ ，同理，查核多項式  $h(X)$  等效於查核矩陣  $H$ 。由矩陣的關連可知  $HG^T = 0$ ，其對應的多項式為

$$g(X)h(X) \bmod (X^n + 1) = 0 \quad (3.19)$$

所以我們可以說生成多項式  $g(X)$  與查核多項式  $h(X)$  均為多項式  $X^n + 1$  的因式，如下所示

$$g(X)h(X) = X^n + 1 \quad (3.20)$$

這個性質提供選擇產生多項式或查核多項式的基礎。我們可以說如果  $g(X)$  為(n-k)幕次多項式且為多項式  $X^n + 1$  的因式，則  $g(X)$  為(n,k)循環碼的產生多項  $h(X)$  為(n,k)循環碼的查核多項式。

### 3.2.2 生成矩陣與查核矩陣

給定一(n,k)循環碼的生成矩陣，我們可以用 k 個多項式  $g(X)$ ， $Xg(X)$ ，...  
 $X^{k-1}g(X)$  展開編碼以建造生成矩陣  $\mathbf{G}$ 。因此以 n 個對應這些多項式的向量為列  
 向量形成  $k \times n$  的生成矩陣  $\mathbf{G}$ 。

如果要建造循環碼的查核矩陣就要謹慎了。首先將(3.20)式乘以  $a(X)$ ，接  
 著用(3.2)式得到

$$c(X)h(X) = a(X) + X^n a(X) \quad (3.21)$$

多項式  $c(X)$  及  $h(X)$  定義在(2.1)式及(3.18)式，在(3.21)式的左側是相乘，所  
 以幕次增至  $n+k-1$ ，而在右側多項式  $a(X)$  的幕次為  $k-1$  或更小，這意味  
 $X^k, X^{k-1}, \dots, X^{n-1}$  並不會出現在(3.21)式的右側，因此  $c(X)h(X)$  的  
 $X^k, X^{k-1}, \dots, X^{n-1}$  的係數為零，我們得到  $n-k$  組方程式

$$\sum_{i=j}^{j+k} c_i h_{k+j-i} = 0 \quad \text{for } 0 \leq j \leq n-k-1 \quad (3.22)$$

比較(3.22)式與  $cH^T = 0$ ，有個重要的結論：在(3.22)式中多項式相乘的查  
 核多項式  $h(x)$  之係數與  $cH^T = 0$  的查核矩陣  $\mathbf{H}$  的係數所排的順序恰好反向。  
 這使得我們定義查核互易多項式 (reciprocal of the parity-check polynomial) 如  
 下：

$$X^k h(X^{-1}) = X^k (1 + \sum_{i=1}^{k-1} h_i X^{-1} + X^{-k}) = 1 + \sum_{i=1}^{k-1} h_{k-i} X^i + X^k \quad (3.23)$$

由(3.23)可看出多項式  $x^k h(x^{-1})$  是  $x^n + 1$  的因式，從  $(n-k)$  個多項式  
 $x^k h(x^{-1}), x^{k-1} h(x^{-1}), \dots, x^{n-1} h(x^{-1})$  就可做為  $(n-k) \times n$  查核矩陣  $\mathbf{H}$  的各列  
 係數。一般生成矩陣  $\mathbf{G}$  與查核矩陣  $\mathbf{H}$  依上述方式建造並不是系統型式，如果  
 要轉換成系統型式，只需要在對應的列做簡單運算即可。

另一種表示訊息位元與查核位元的方式為，令  $\mathbf{H}$  表示  $(n-k) \times n$  矩陣，定義如下

$$\mathbf{H} = [P^T | I_{n-k}] \quad (3.24)$$

$P^T$  代表  $(n-k) \times k$  矩陣，它為矩陣  $\mathbf{P}$  的轉換 (transpose) 矩陣而  $I_{n-k}$  為  $(n-k) \times (n-k)$  單位矩陣，因此可以寫成

$$\mathbf{H}\mathbf{G}^T = [P^T | I_{n-k}] \begin{bmatrix} I_k \\ P^T \end{bmatrix} = P^T + P^T$$

在以 2 為基底的運算裡  $P^T + P^T = 0$ ，0 代表  $(n-k) \times k$  零矩陣 (所有的元素皆為零)，所以

$$\mathbf{H}\mathbf{G}^T = 0 \quad (3.25)$$

也可以寫成  $\mathbf{G}\mathbf{H}^T = 0$ ，若在(3.14)式前面乘以  $\mathbf{H}^T$ ，再用(3.25)式可得到

$$\mathbf{c}\mathbf{H}^T = \mathbf{m}\mathbf{H}\mathbf{G}^T = 0 \quad (3.26)$$

徵狀具有兩種重要的性質，一是徵狀和誤差圖樣有關。要證明這個性質，首先用(3.15)式及(3.17)式，接著用(3.26)式可得(3.27)式，因此查核矩陣  $\mathbf{H}$  允許我們計算徵狀  $\mathbf{s}$ ，它的確僅與誤差圖樣  $\mathbf{e}$  有關。

$$\mathbf{s} = (\mathbf{c} + \mathbf{e})\mathbf{H}^T = \mathbf{c}\mathbf{H}^T + \mathbf{e}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T \quad (3.27)$$

另一個特性是所有誤差圖樣依編碼字的不同，也擁有相對的徵狀。以  $k$  訊息位元而言，有  $2^k$  種編碼向量如  $\mathbf{c}_i$ ， $i = 0, 1, \dots, 2^k - 1$ ，對應的任意誤差圖樣  $\mathbf{e}$  也有  $2^k$  種如下式

$$\mathbf{e}_i = \mathbf{e} + \mathbf{c}_i \quad i = 0, 1, \dots, 2^k - 1 \quad (3.28)$$



### 3.3 模擬分析

在探討縮短循環碼硬體設計之前，本章節將使用 Matlab 軟體進行循環碼的錯誤更正能力模擬，並針對在不同的通道下，是否能達到本文所要求的更正錯誤能力。另外再針對錯誤圖樣的部分去分析徵狀對解碼能力的影響，因此在此章節將針對這兩部分加以模擬。

首先編碼部分採用 3.1 節提出的編碼方式，並使用二階相位偏移調變 (Binary Phase Shift Keying, BPSK) 進行訊號調變，加上兩種通道作為干擾雜訊，第一種是白高斯雜訊，第二種是白高斯雜訊加上突發連續錯誤。在接收端的部分，採用 3.2 節所提出的徵狀運算解碼，並且針對錯誤圖樣去分析無法更正錯誤的原因。

#### 3.3.1 錯誤圖樣

在 3.2 節裡提出的徵狀解碼原理，可以看出徵狀  $s$  的計算和錯誤圖樣  $e$  有很大的相關性。因此，可以利用徵狀去判別資料位元錯誤在第幾個位元。

表 3.1 錯誤位元與徵狀比對表

錯誤位元	徵狀(syndrome)	錯誤位元	徵狀(syndrome)	錯誤位元	徵狀(syndrome)
1	1000000000	10	0000000001	19	0110111011
2	0100000000	11	1011011100	20	1000000001
3	0010000000	12	0101101110	21	1111011100
4	0001000000	13	0010110111	22	0111101110
5	0000100000	14	1010000111	23	0011110111
6	0000010000	15	1110011111	24	1010100111
7	0000001000	16	1100010011	25	1110001111
8	0000000100	17	1101010101	26	1100011011
9	0000000010	18	1101110110		

由表 3.1 中可以看出錯誤位元的徵狀情況，舉例來說，以 16 位元的資料來說，假設原始資料是 0000000000000001，經由系統生成矩陣運算出傳送資料為 00000000000000010110111001，而在資料傳送的途中受到雜訊的干擾，產生了錯誤序列 0000000000000000001000000，使得接收端收到的接收資料為 00000000000000010111111001，經由 3.16 式運算出來的徵狀是 1000000001，在與表 3.1 去做徵狀比對，便可知道錯誤位元是在第 20 個位元。解碼器變是利用這方法去進行更正資料。若資料錯誤兩個位元的話，則算出來的徵狀會是兩個徵狀互相互斥或運算(Exclusive-OR)，例如錯誤圖樣為第一位元和第 11 位元，則算出來的徵狀會是 0011011100，如式(3.31)。以此類推，三個錯誤、四個錯誤…等等，皆是這種方式產生。

$$1000000000 \oplus 1011011100 = 0011011100 \quad (3.31)$$

但是此種方式卻有兩種情況下會造成無法判別錯誤圖樣，而導致無法正確的更正錯誤資料。情況一是徵狀重複導致偵測器無法判別是哪個位元錯誤。舉例來說，錯誤圖樣為第一個位元和第 10 個位元時，用式(3.29)計算出來的徵狀是 1000000001，當偵測器要去比對徵狀時，卻發現錯誤圖樣為第 20 位元時的徵狀是相同的，此時偵測器便會誤判錯誤位元為第 20 位元，進而去更正第 20 位元的資料，使得資料錯誤由原本錯誤 2 個位元變成錯誤 3 個位元；情況二則是兩個錯誤相隔 5 個位元以上，則偵測器無法判別錯誤位元，以傳統的偵測器硬體架構來說，當徵狀暫存器最左的五個排列都為零，而且暫存器最右邊的五個排列位元為最大長度，此時便有可能發生錯誤，若兩個錯誤相間超過 5 個位元的話，則無法正確的更正錯誤了。

圖 3.5 是針對情況一的部分去進行模擬，利用 Matlab 程式去計算徵狀的排列組合有多少是重複的，而造成偵錯器判別錯誤。橫軸是徵狀重複的百分比；縱軸則是兩種錯誤圖樣的排列組合，一種是 1-bit~5-bit 的隨機錯誤(error ~ error5)，另一個則是 1-bit~5-bit 的連續突發錯誤(1 bit-burst ~ 5 bit-burst)。由下圖可以看出一到五位元的連續突發錯誤徵狀重複的機率是 0%，表示連續突發錯誤能力是良好的，都能夠正確的把資料還原回來；另一個隨機錯誤徵狀的部分便有重複的機會。

此循環碼的最小漢明距離為 3，因此每次的徵狀運算後都只能更正一個位元，又因縮短循環碼具有良好的突發性錯誤更正能力，故在而後章節會做一套解碼到六套解碼的錯誤更正能力模擬。

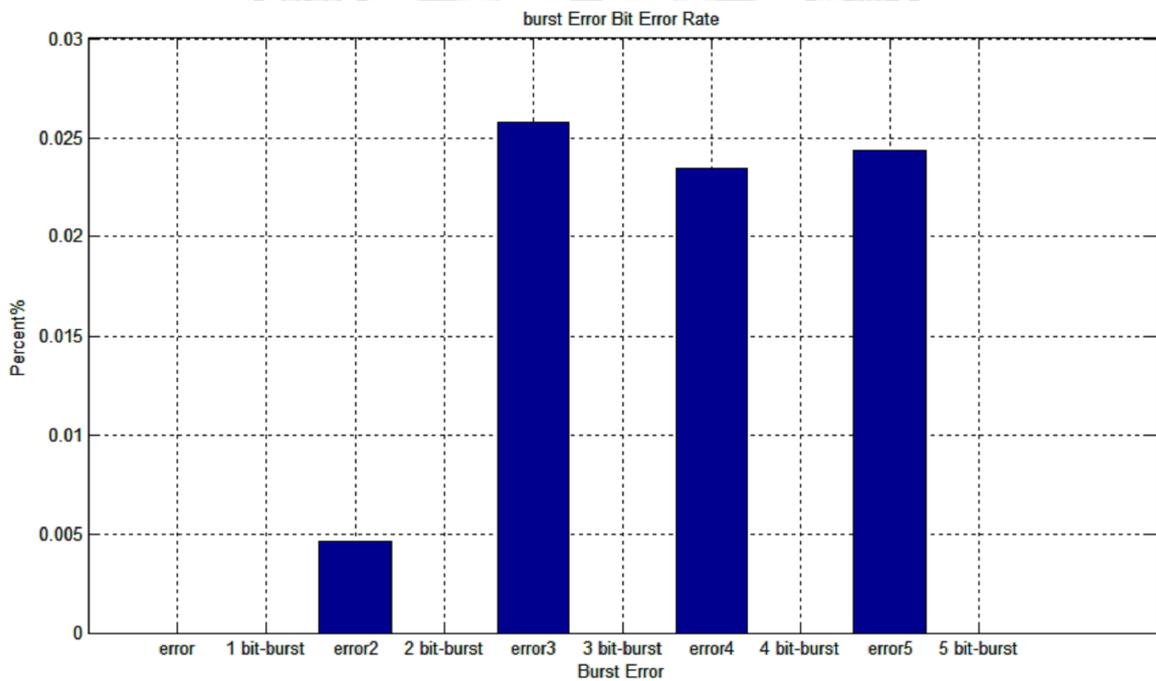


圖 3.5 徵狀重疊模擬數據

### 3.3.2 錯誤更正能力

在這章節，首先進行循環碼在不同的通道下之錯誤更正能力，經過 Matlab 模擬得到圖 3.6 和圖 3.7。位元錯誤率(Bit Error Rate, BER)是總錯誤位元與總資料位元的比值，BER 越低，代表錯誤位元越少。此模擬的調變系統是使用 BPSK。BPSK 的位元錯誤率在白色高斯雜訊(AWGN)下表示之公式如式(3.32)。

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \quad (3.32)$$

由圖 3.6 可以觀察到此縮短循環碼的錯誤更正能力，藍色的線條是有加錯誤更正碼的資料，而紅色的線是未加錯誤更正碼的，可以看到在 BER=10<sup>-4</sup> 時，解碼增益值(coding gain)為 2.4dB，優於未加錯誤更正碼的曲線，因此證明循環碼可應用於無線通訊系統之錯誤更正碼。

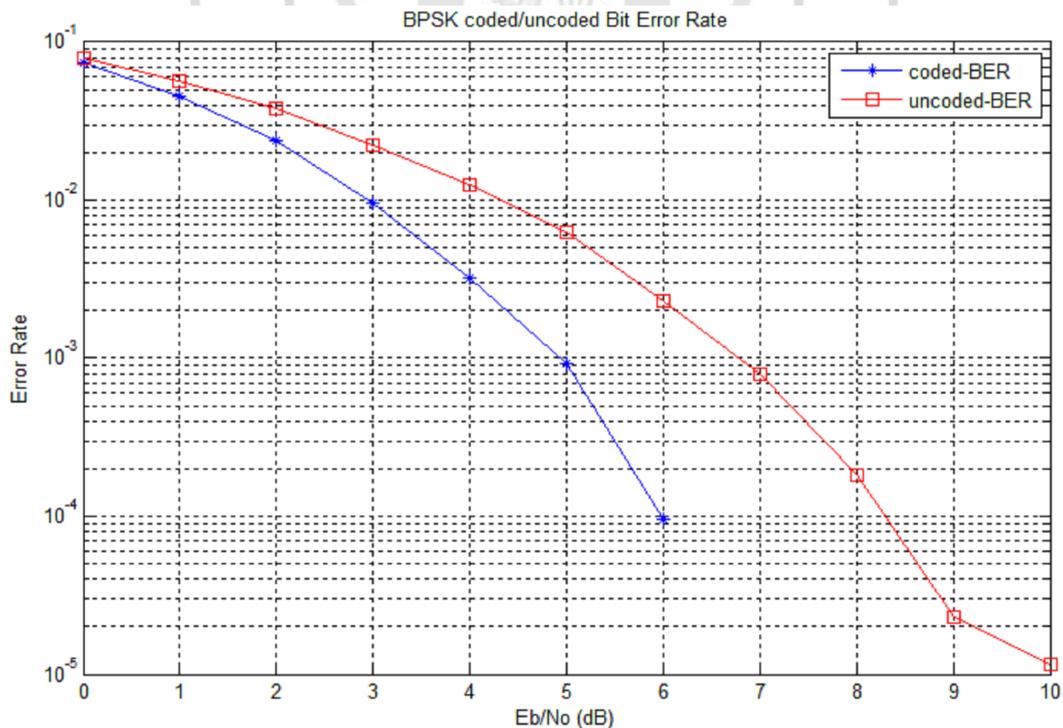


圖 3.6 縮短循環碼在 AWGN 通道裡的 BER 模擬

接下來分析循環碼在 AWGN 與突發性隨機錯誤(random burst error)通道裡的錯誤更正能力，圖 3.7 是突發性隨機錯誤的示意圖。在圖 3.8 到圖 3.10 是縮短循環碼在不同位元隨機突發性錯誤通道中的 BER 模擬， $E_b/N_0 = 10\text{dB}$ 之前受到 AWGN 和 random burst error 的雜訊干擾；10dB 之後只有受到 random burst error 雜訊干擾，因此可以看出一到六次疊代循環碼解碼對於突發性錯誤有良好的錯誤更正能力。

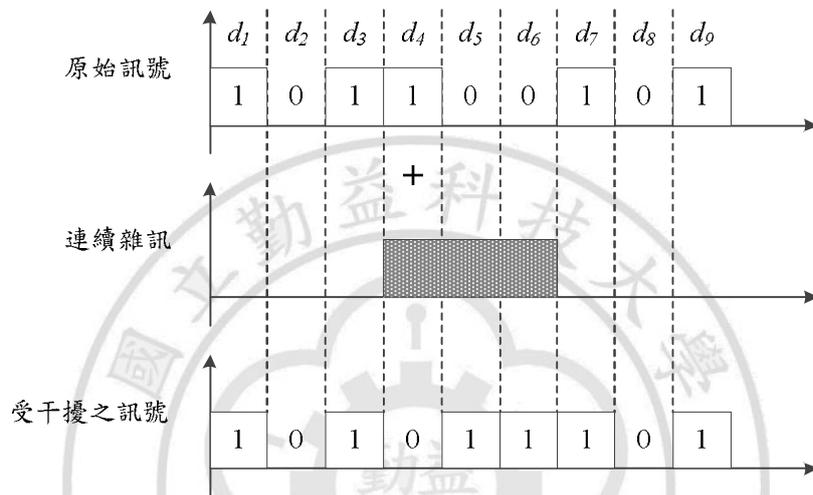


圖 3.7 隨機突發性錯誤(random burst error)示意圖

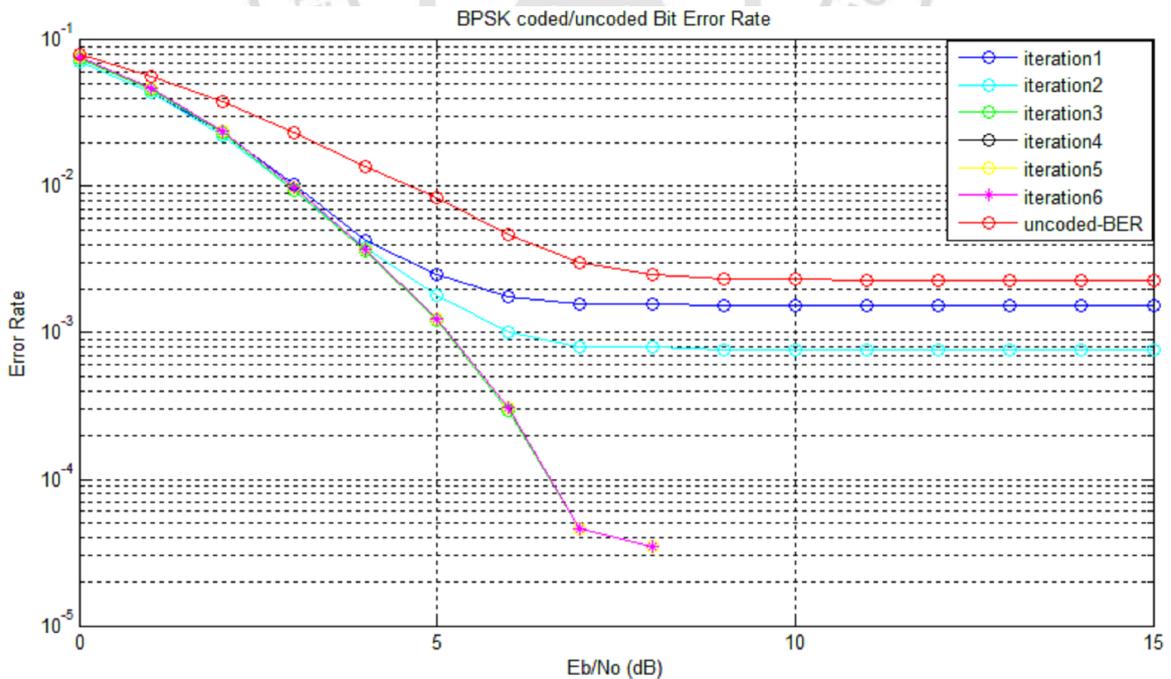


圖 3.8 3-bit burst error 通道裡的 BER 模擬

由圖 3.8 和圖 3.9 之中可以看出隨機突發性錯誤只要不超過解碼疊代次數，此解碼器便可以將資料正確的還原回來。若隨機突發錯誤超過疊代次數的話，如圖 3.10，則完全無法解碼回來。

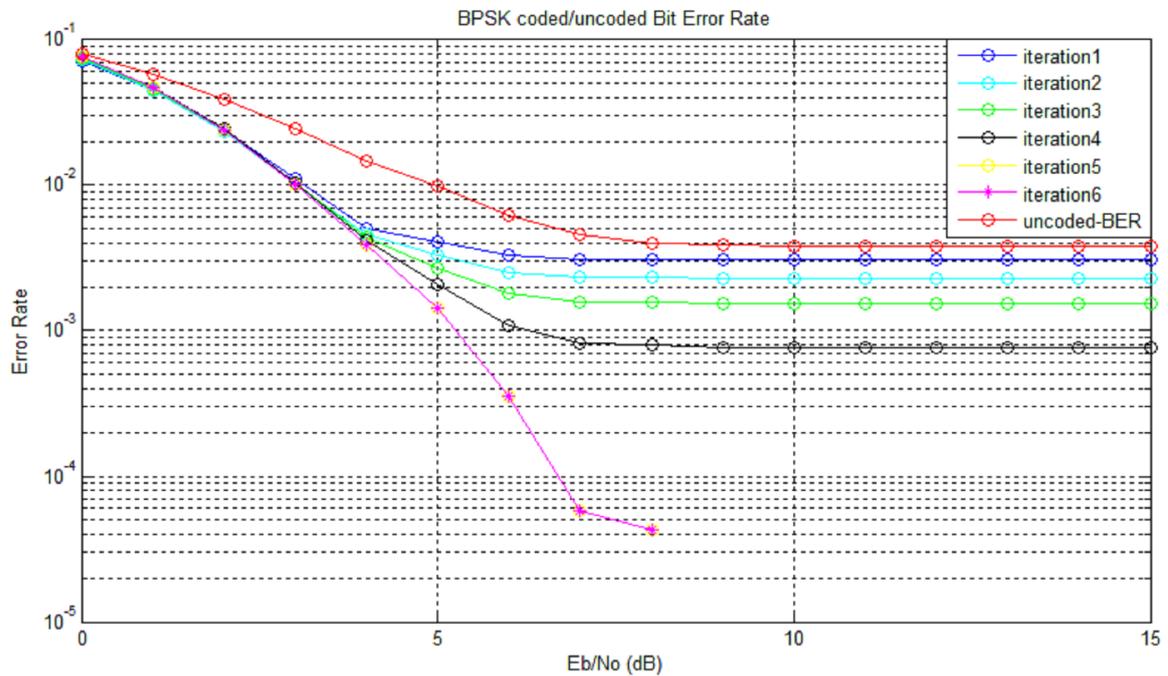


圖 3.9 5-bit burst error 通道裡的 BER 模擬

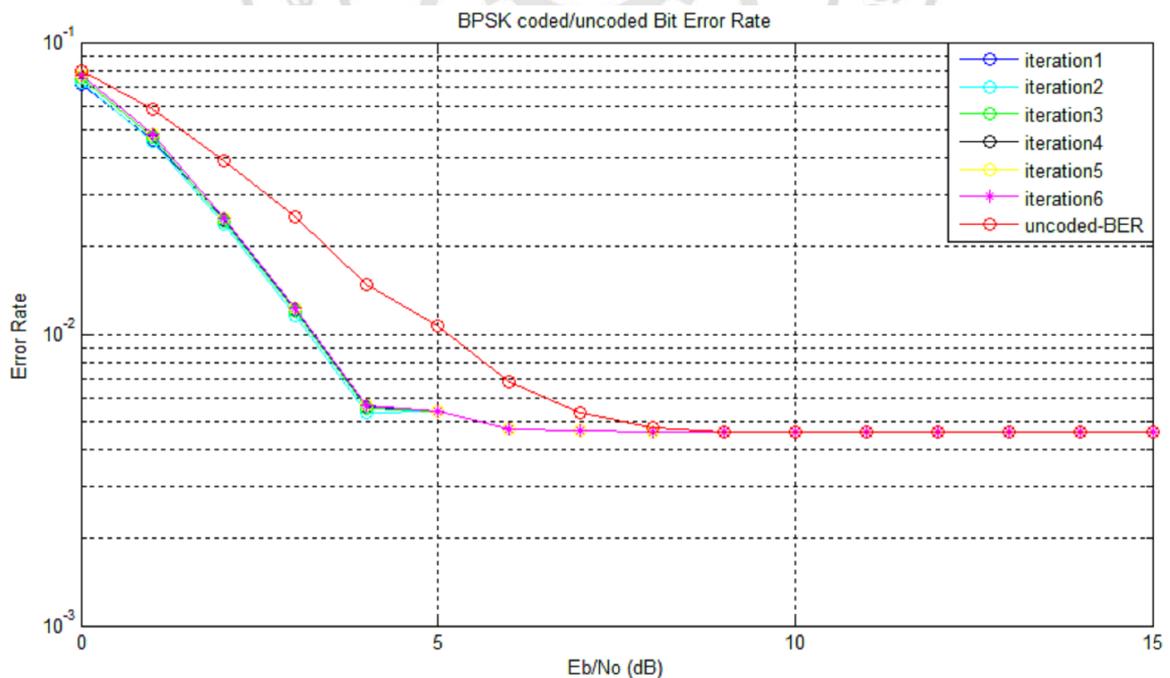


圖 3.10 6-bit burst error 通道裡的 BER 模擬

## 第四章 縮短循環碼硬體編解碼架構

在前一章節介紹縮短循環碼的編碼與解碼原理，並且利用 Matlab 軟體去進行演算法與系統的模擬，也達到我們的需求。本章節將分別描述縮短循環碼的編碼與解碼之傳統式串列硬體架構，以及本文所提出新的並列式硬體架構設計，並且說明系統架構與晶片硬體實現的結果。

### 4.1 設計流程

數位 IC 的設計流程可以分為兩個部分，一個是軟體模擬的部分，另一個則是硬體合成的部分。軟體的部分，本研究主要是使用 Matlab 來進行縮短循環碼解碼和編碼的演算法模擬，利用第二章節所提出的演算法進行功能與定點的模擬，並且達到系統的要求。

硬體部分，首先利用硬體描述語言(Verilog hardware description language, Verilog-HDL)實作硬體設計，Verilog 是為了製作數位電路而用來描述特殊應用積體電路和現場可程式邏輯閘陣列的設計之用。當硬體程式完成之後，經由 NC-verilog 進行波形模擬，並且查看是否達到我們預期設計的條件。確定之後，便使用國家晶片設計製作中心(Chip Implementation Center, CIC)裡的合成與佈局軟體去完成硬體電路。主要會使用到 Design compiler (DC)和 IC Compiler (ICC)這兩套軟體去完成。DC 主要的功能是将寫好的 Verilog 或 VHDL Code 轉成 Gate-Level Netlist，此外還可以搭配 Synopsys 已設計好的 Design Wave Library 直接套用到自己的 Design，可以大幅度減少開發時間。而 ICC 則是將 Gate-Level Netlist 去進行實體合成、時脈樹合成、繞線、良率最佳化與簽證(sign-off)相互關聯性整合。設計流程如圖 4.1 所示。

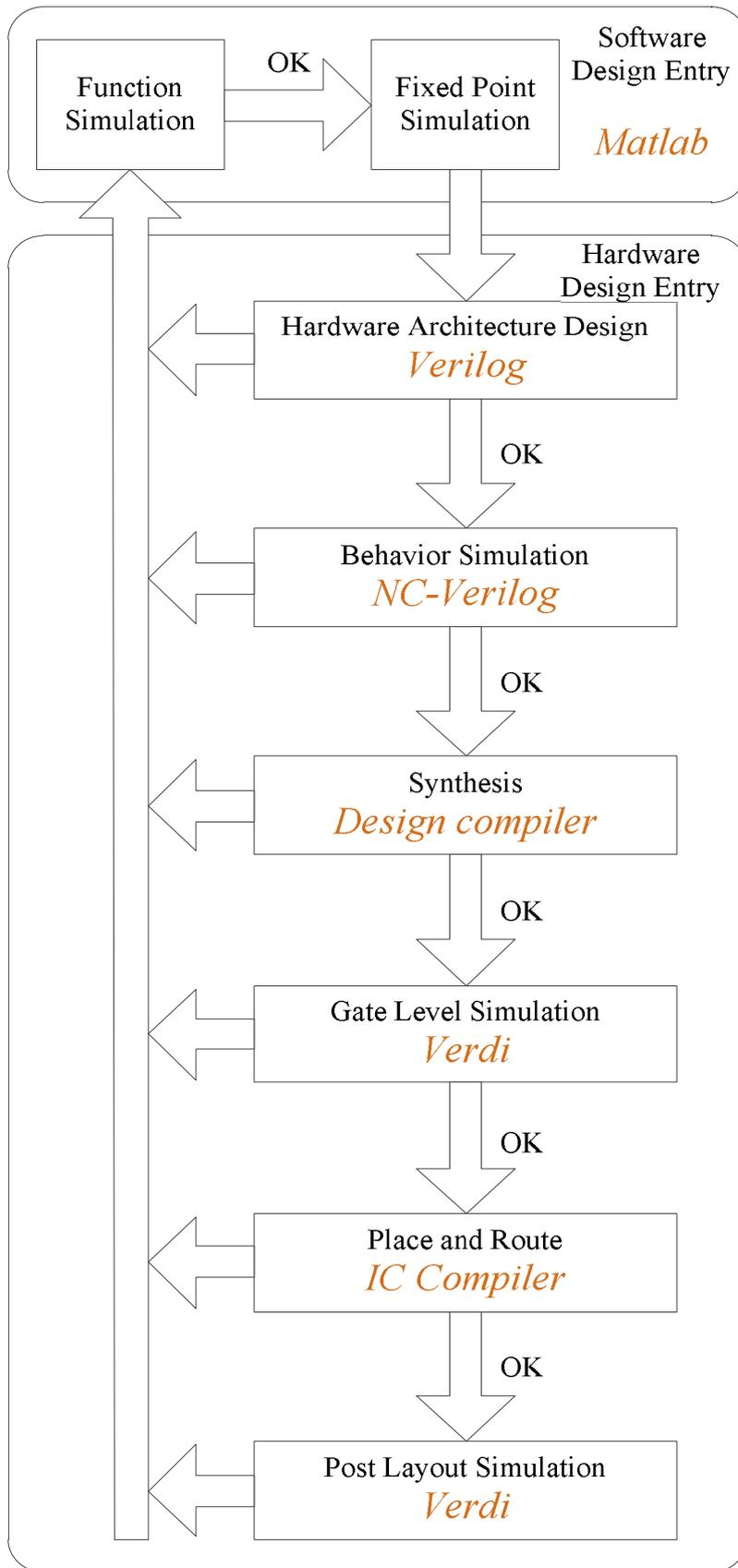


圖 4.1 演算法與硬體實現流程圖

## 4.2 縮短循環碼編碼硬體架構

在 3.1 章節裡面所提到的演算法，根據式(3.4)，編碼多項式是由 16 位元的資料和 10 位元經由除法運算所剩下的餘數所組成的，因此傳統式的縮短循環碼編碼電路是利用移位暫存器設計出除法電路，如圖 4.2 說明一個對傳送 26 位元為一區塊編碼的移位暫存器的配置。

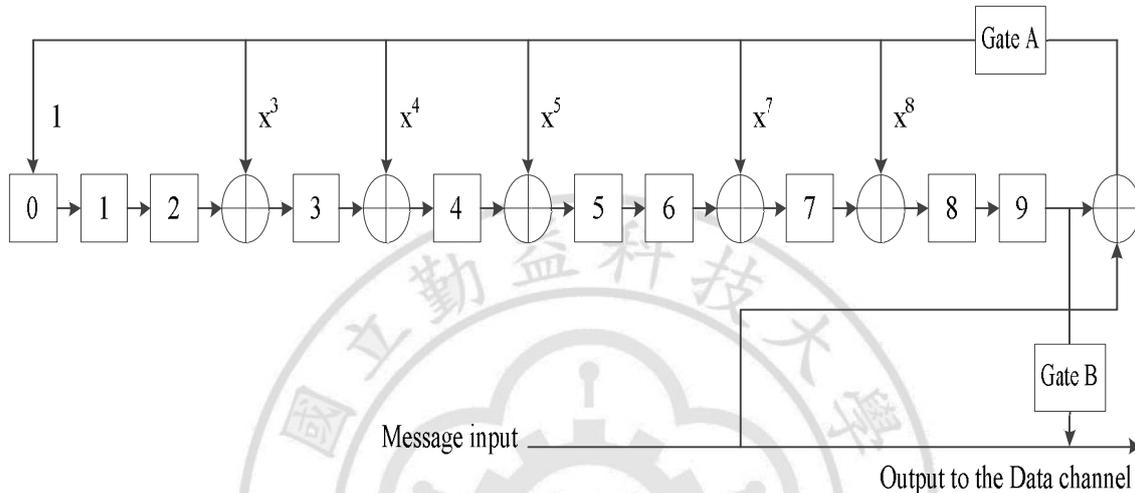


圖 4.2 移位暫存器之編碼電路

編碼步驟如下：

- (1) 在每一個區塊的起始,將 10 位元編碼暫存器皆清除為零的狀態。
- (2) 將 A,B 閘打開(資料通過), 16 位元串列傳輸連續進入編碼並和資料輸出至通道同步計數。
- (3) 整個區塊 16 個傳輸位元都被送入後,A,B 閘關閉。
- (4) 編碼移位暫存器再移位 10 次檢測字組，並接續在資料位元之後形成 26 個編碼位元，再逐一輸出資料至通道。
- (5) 下一區塊之編碼則重複此循環步驟。

本研究的縮短循環碼編碼電路是使用 10 個移位暫存器去設計出來的，優點是功率消耗小、面積小，可是缺點是運算時間太久，編碼一筆 16 位元的原始資料，並且輸出 26 位元的傳送資料時，需要 26 個 clock 的時間才有辦法完成單筆資料的編碼運算，原因是資料輸入方式是串列式 1 位元輸入，每個 clock 輸入單筆 1 位元資料，因此輸入 16 位元的資料則需要 16 個 clock，當資料完全進入之後，在經過 10 個 clock 的運算與資料輸出，才能得到 26 位元的資料，故在處理的時間會比較長一點。

本文提出了並列式編碼邏輯運算架構，可降低運算時間與提高資料的吞吐量，此架構的設計理念主要是參考 3.1 章節裡式(3.9)的係數矩陣  $\mathbf{P}$ ，把矩陣  $\mathbf{P}$  每行的 0 或 1 當作是一個開關，以控制資料的輸入與否，0 代表開關關閉，資料不輸入；1 代表開關開啟，資料可以輸入作運算，如圖 4.3。因為資料的產生是利用模 2 的加法運算去計算出來的，如式(3.13)所示，一筆 16 位元的原始資料與  $16 \times 26$  的系統生成矩陣做互斥或 (Exclusive-OR) 運算便可以產生 26 位元的傳送資料，利用此特性去設計出此並列式編碼電路。此電路可在一個 clock 的時間將單筆 16 位元的資料完成編碼，並且加上後面 10 個檢查位元，成為可以傳送的 26 位元資料。

$$\mathbf{P} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

圖 4.3  $16 \times 10$  係數矩陣。

實際電路的硬體架構如圖 4.4 所示， $a\_in[15] \sim a\_in[0]$  是原始資料的輸入端， $a\_in[15]$  為資料的最高位元， $a\_in[0]$  為資料的最低位元。因為傳送的資料格式是在原始資料後面在加上 10 個位元的檢查位元，所以  $a\_in[15] \sim a\_in[0]$  被送入邏輯閘運算之後，會在輸出端完整的輸出 16 位元資料。而檢查位元的部分，則依造上述的設計方式去設計，以 Logic gates 1 的部分為例， $P$  係數矩陣的第一行是  $[0111110000111110]$ ，1 代表資料有輸入，因此  $a\_in[14] \sim a\_in[10]$  就會有資料輸入到互斥或閘去做 mod 2 的加法運算，運算完成之後，便會輸出  $c_9$  成為最高位元的檢查位元了，以此類推，每筆資料進去不同的 Logic gates 並且去做運算，便可以在一個 clock 的時間內完成編碼，運算的時間減少了百分之九十三。

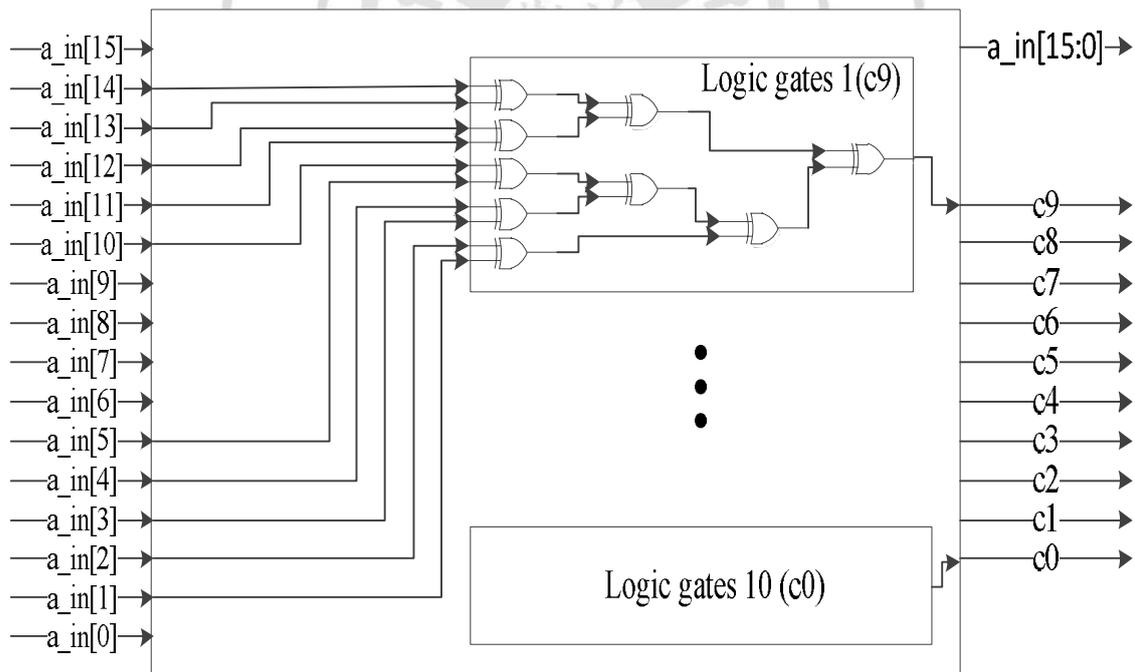


圖 4.4 改良編碼並列式硬體電路架構

### 4.3 縮短循環碼解碼硬體架構

在第 3.2 章節裡面所提到的解碼演算法，主要是經由計算徵狀，並且去進行錯誤圖樣比對而完成解碼的動作。圖 4.5 為傳統式的移位暫存器解碼電路，主要是利用移位除法電路計算徵狀，再經由偵測邏輯判別錯誤位元，更正錯誤位元的資料。

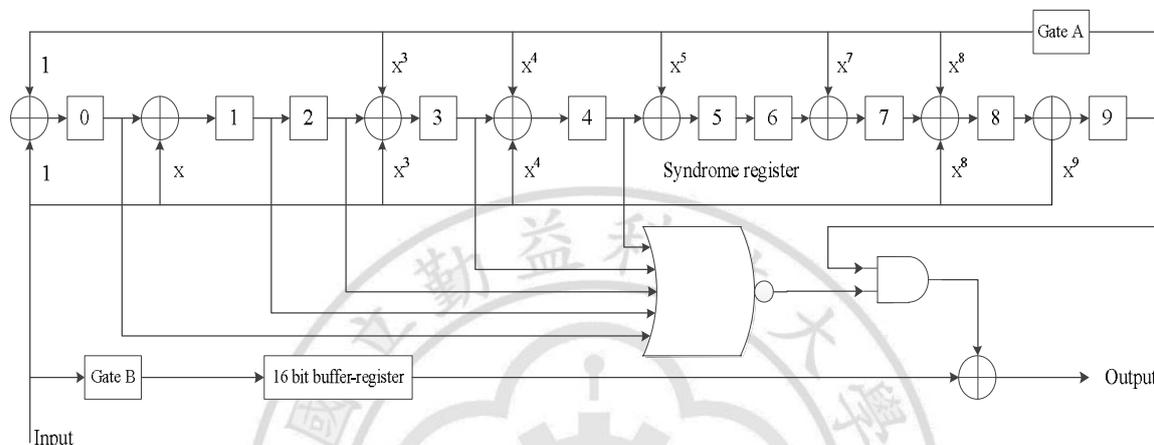


圖 4.5 移位暫存器之解碼電路

解碼步驟如下：

- (1) 在每個區塊起始將 10 位元 syndrome 暫存器和 16 位元緩衝暫存器皆清除為零的狀態。
- (2) 16 個資料位元被分給 syndrome 及緩衝暫存器.將 A、B 閘打開(傳送)。
- (3) 將 B 閘關閉並且將 10 個檢測位元送入 syndrome 暫存器。
- (4) 在緩衝暫存器的 16 個資料位元被輸出，並滿足一組同時存在暫存器轉態時，A 閘是被打開的。
- (5) 當在 syndrome 暫存器最左的五個排列皆為零，而且在暫存器最右的五個排列位元為最大長度,此時便有可能會有錯誤發生。
- (6) 關閉 A 閘，從緩衝暫存器移位串連加入資料與 syndrome 暫存器作互斥或運算，並更正錯誤資料位元。
- (7) 循環重複下一個 block。

本研究的縮短循環碼解碼電路由 10 個除法移位暫存器和邏輯偵測電路組合而成，優點跟編碼一樣，功率消耗低、面積小，但是依然運算時間非常久，傳統式電路需要 42 個 clock 的時間去做運算，其中的 26 個 clock 是將 26 位元資料送入 syndrome 暫存器做徵狀運算，另外的 16 個 clock 是計算錯誤圖樣，並且利用邏輯偵測器去更正錯誤的資料，結束之後便會輸出原始的 16 位元資料。

為了縮短電路的運算時間，本文提出並列式解碼邏輯運算架構，主要可以分成兩個部分來作討論。第一部分為徵狀的計算，設計概念跟編碼的架構是差不多的，主要是利用系統查核矩陣的轉置矩陣，如圖 4.6 去做設計，因為由 3.2 章節的式(3.28)可以知道徵狀跟錯誤序列式有關係的，所以藉由簡單的互斥或閘，便可以知道錯誤圖樣為多少了。

$$\mathbf{H}^T = \begin{bmatrix}
 1000000000 \\
 0100000000 \\
 0010000000 \\
 0001000000 \\
 0000100000 \\
 0000010000 \\
 0000001000 \\
 0000000100 \\
 0000000010 \\
 0000000001 \\
 1011011100 \\
 0101101110 \\
 0010110111 \\
 1010000111 \\
 1110011111 \\
 1100010011 \\
 1101010101 \\
 1101110110 \\
 0110111011 \\
 1000000001 \\
 1111011100 \\
 0111101110 \\
 0011110111 \\
 1010100111 \\
 1110001111 \\
 1100011011
 \end{bmatrix}$$

圖 4.6 系統查核矩陣的轉置矩陣

實際的徵狀運算硬體電路如圖 4.7 所示， $c\_in[25] \sim c\_in[0]$  是接收資料的輸入端， $c\_in[25]$  為資料的最高位元， $c\_in[0]$  為資料的最低位元。以 Logic gates 1 的部分為例，查核矩陣轉置矩陣的第一行是 [10000000001001111101100111]，1 代表資料有輸入，因此  $c\_in[25] \sim c\_in[10]$  就會有資料輸入到互斥或閘做 mod 2 的加法運算，運算完成之後，便會輸出  $s_9$  成為最高位元的徵狀，以此類推，每筆資料經由不同的 Logic gates 運算，便可以在一個 clock 的時間內完成徵狀的計算。運算時間從 26 個 clock 縮短到 1 個 clock，整整減少了百分之九十六的運算時間。

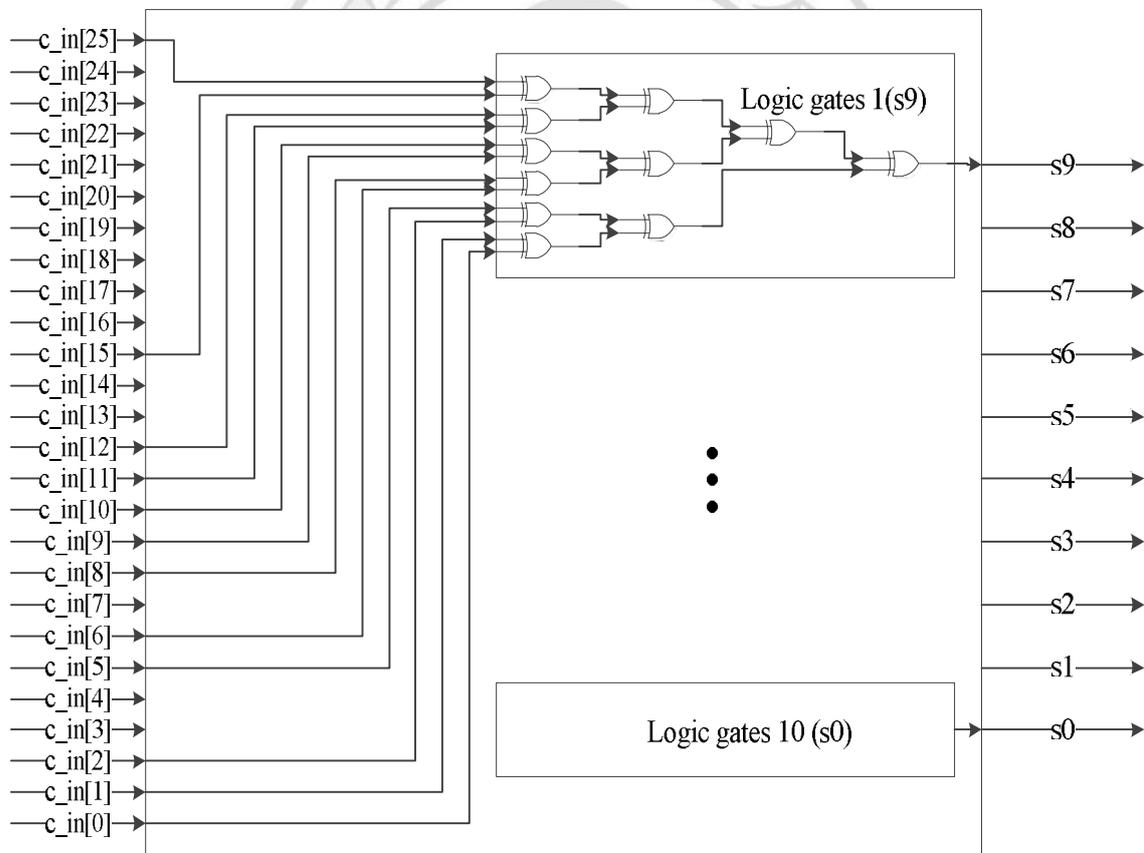


圖 4.7 改良式徵狀運算並列式硬體電路架構

第二部分則是偵測邏輯， $g(x)$ 除法電路計算徵狀的電路有一個很重要的特點。若 $s(x)$ 是 $r(x)$ 的徵狀式，則 $r(x)$ 的循環移位  $xr(x)$  (在  $\text{mod } x^n - 1$  運算下)的徵狀是  $s_1(x)$ ，是 $s(x)$ 在徵狀計算電路中無輸入時右移一位的結果，級如下式：

$$s_1(x) \equiv xs(x) \pmod{g(x)} \quad (4.1)$$

由徵狀式定義可知  $xr(x)$  的徵狀式為

$$s_1(x) \equiv xr(x) \pmod{g(x)} \equiv x\bar{y}(x) + q_1(x)g(x) \quad (4.2)$$

$$xs(x) \equiv x\bar{y}(x) + xq(x)g(x) \quad (4.3)$$

兩式相減可得到：

$$xs(x) - s_1(x) \equiv g(x)(xq(x) - q_1(x)) \equiv 0 \pmod{g(x)} \quad (4.5)$$

因此

$$s_1(x) \equiv xs(x) \pmod{g(x)} \quad (4.6)$$

徵狀計算電路特性，在循環碼解碼運算中非常的有用。若 $c(x)$ 是循環碼 $c$ 的其中一個碼字，則 $xc(x) \in c$ 。因此，若  $s(x) \equiv e(x) \pmod{g(x)}$  是  $r(x) = c(x) + e(x)$  的徵狀式，則  $xs(x) \equiv xe(x) \pmod{g(x)}$  就是  $xr(x) = xc(x) + xe(x)$ ，也就是說若  $e(x)$  是一個可糾正的錯誤圖樣，則  $e(x)$  的循環移位  $xe(x)$  也是一個可糾錯的錯誤圖樣，一般來說  $x^i e(x), (1 \leq i \leq n-1)$  也是可糾錯的錯誤圖樣。



表 4.1 的錯誤圖樣偵錯電路演算法左邊區塊一種徵狀的排列組合演算法，而右邊則是 2 種徵狀的排列組合演算法，此演算法共有 10 個排列組合的比較，並且比對出最節省邏輯閘，又可以達到偵錯功能的條件。利用上列的演算法，並可以設計出圖 4.8 的改良式偵測錯誤並列式硬體電路架構。

傳統的電路是使用移位暫存器，若要計算出 16 位元的錯誤圖樣並且去做更正，需要 16 個 clock 去做計算，改良式電路只需要 1 個 clock 便可以將 16 位元的錯誤圖樣計算出來並且更正成原始的資料。可以看到輸入端為  $c\_in[15:0]$  和上一級徵狀計算電路所得到的徵狀  $s_9 \sim s_0$ ，輸入到每一個位元各個不同的邏輯偵測電路，並且計算出錯誤圖樣  $e_{15} \sim e_0$ ，再與  $c\_in[15:0]$  作互斥或運算，便可以得到原始的資料了。以 Logic gates 1 舉例說明，錯誤圖樣  $e_{15}$ 、 $e_{14}$ 、 $e_{13}$  若以布林代數去表示的話，則會如 (4.7) 式：

$$\begin{aligned}
 e_{15} &= \overline{s_0 + s_1 + s_2 + s_3 + s_4} \cdot s_9 \\
 e_{14} &= \overline{s_0 + s_1 + s_2 + s_3 + s_9} \cdot s_8 \\
 e_{13} &= \overline{s_0 + s_1 + s_2 + s_9 + s_8} \cdot s_7
 \end{aligned}
 \tag{4.7}$$

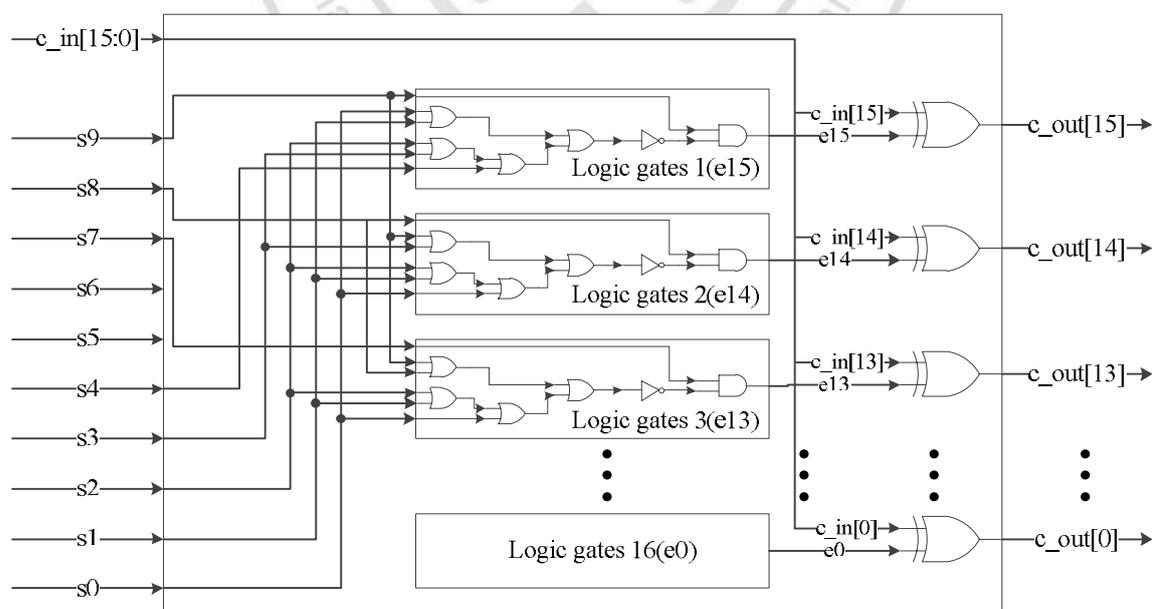


圖 4.8 改良式偵測錯誤並列式硬體電路架構

## 4.4 晶片硬體架構

此晶片具有兩種操作狀態，一種是快速編碼，另一個則是快速解碼，輸入端以及輸出端則是各別使用 16 位元和 26 位元的 Buffer 暫存器去儲存資料。編碼架構如圖 4.9 所示，而解碼架構則是由五套解碼電路組成，因為循環碼對於連續錯誤(burst error)具有相當良好的更正能力，每一套偵錯電路只能更正一個位元的錯誤，故串連了 5 套，使其能解碼連續 5 個位元的錯誤。

此晶片具有 22 個輸入腳位，其中包含 16 位元資料輸入(Chip\_in)，清除(rst)，時脈訊號(clk)，測試腳(test\_mode, test\_se)，資料輸入開關(start)，狀態選擇(state); 還具有 16 位元的輸出腳位(Chip\_out);另外還有 10 位元的輸入輸出雙向腳位(Chip\_io)，當狀態等於 0 時，為編碼狀態，Chip\_io 會當輸出腳做使用，若狀態等於 1 時，為解碼狀態，Chip\_io 會當輸入腳做使用。

其中我們將 Chip\_in、Chip\_out 裡面的最高位元設定為 scan chain，主要作用要在測試模式時用來測試晶片的電路是否正確無誤，此設計總共串連了 342 個 Flip-Flop，而 uncollapsed fault coverage 為 100%。

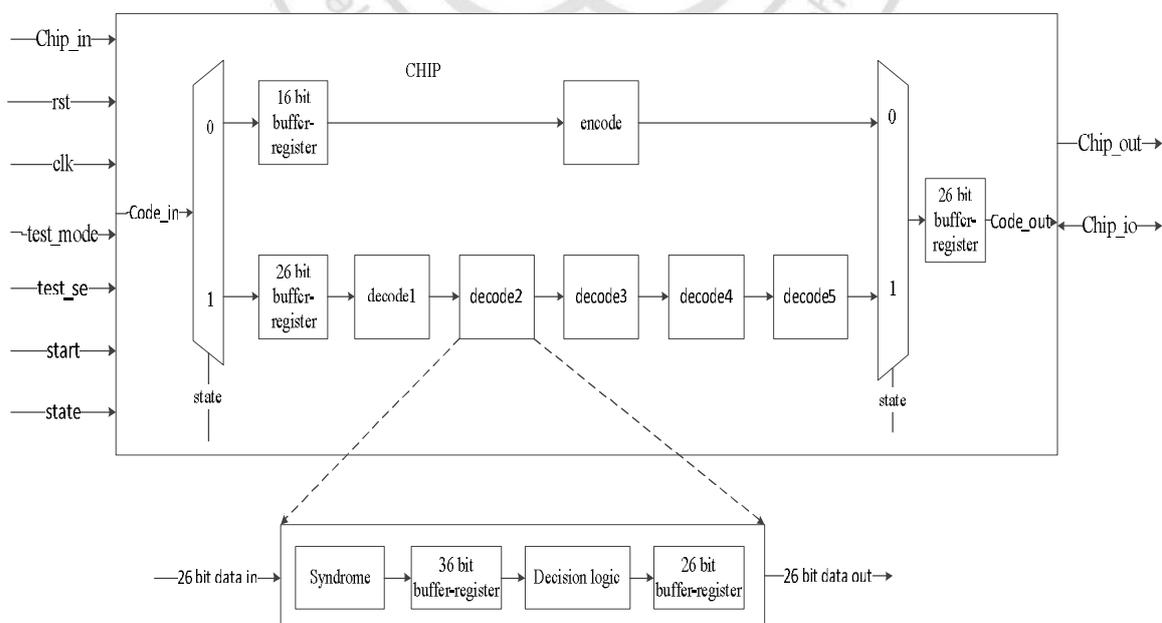


圖 4.9 晶片系統架構圖

## 4.5 硬體實現結果

使用 Verilog-HDL 來描述縮短循環碼的硬體架構，其模擬結果如圖 4.10 (encode)和圖 4.11 (decode)，使用 Cadence 公司所提供的 NC-verilog 做硬體電路的設計；合成的模擬結果如圖 4.12 (encode)和圖 4.13 (decode)，使用 Synopsys 所提供的 Design compiler 做電路的合成，比較圖 4.10 和圖 4.12 可以發現編碼合成前和合成後的功能具有一致性，而圖 4.11 和圖 4.13 也可以發現解碼在合成前和合成後的功能也是一樣的，因此代表合成正確。

最後再使用 Synopsys 所提供的 IC compiler 做電路的佈局，晶片面積為  $1.048 \times 1.048 \text{ mm}^2$ ，預估的功率消耗則為 27mW，操作頻率為 100MHz，並且再次功能驗證，如圖 4.14 (encode)和圖 4.15 (decode)所示，比較圖 4.10 和圖 4.14，發現結果完全正確，而圖 4.11 和圖 4.15 也是一樣的結果，圖 4.16 為晶片佈局設計圖，表 4.2 為晶片預期規格表。

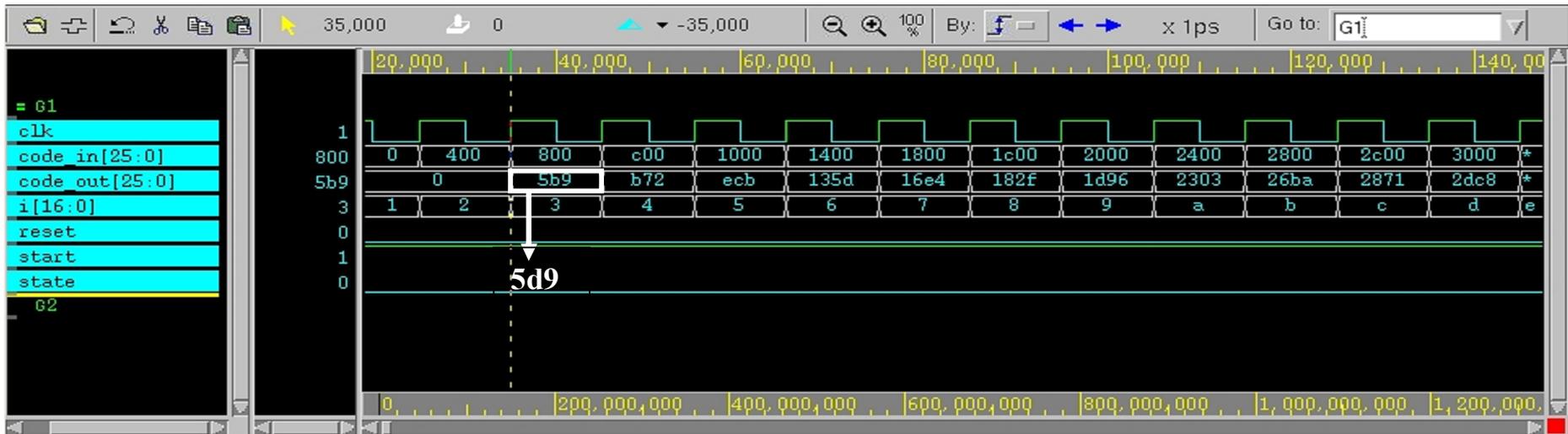


圖 4.10 編碼器 RTL 模擬結果

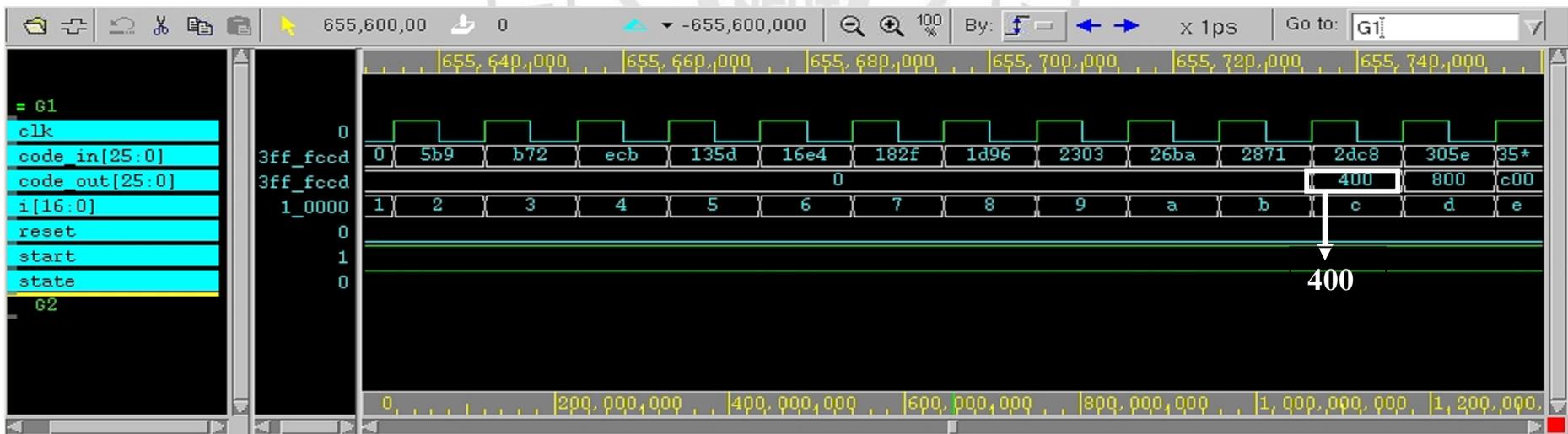


圖 4.11 解碼器 RTL 模擬結果

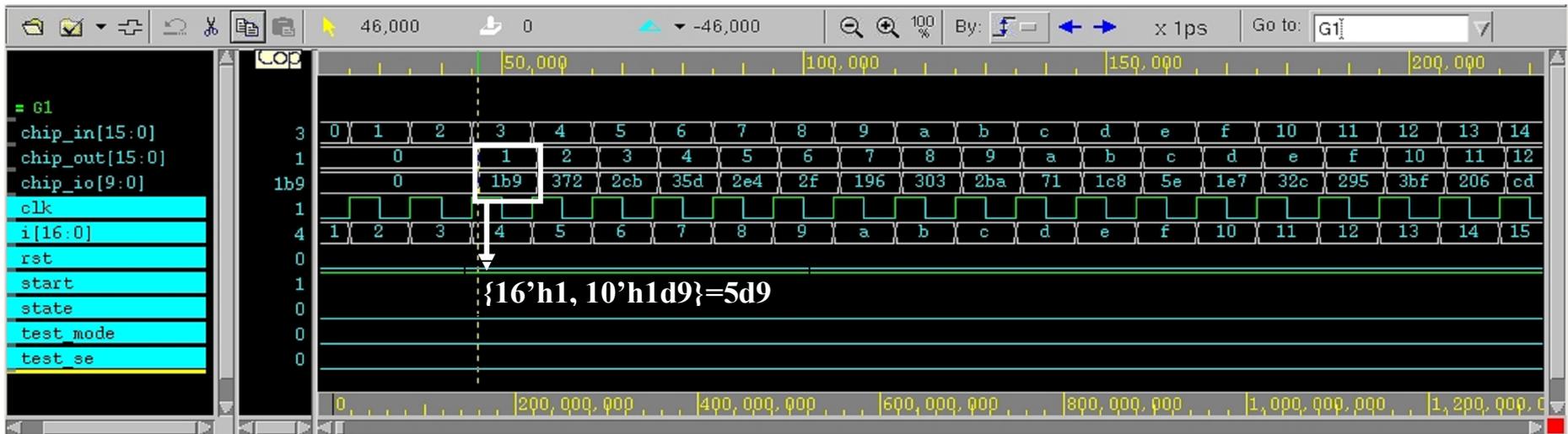


圖 4.12 編碼器合成後模擬結果

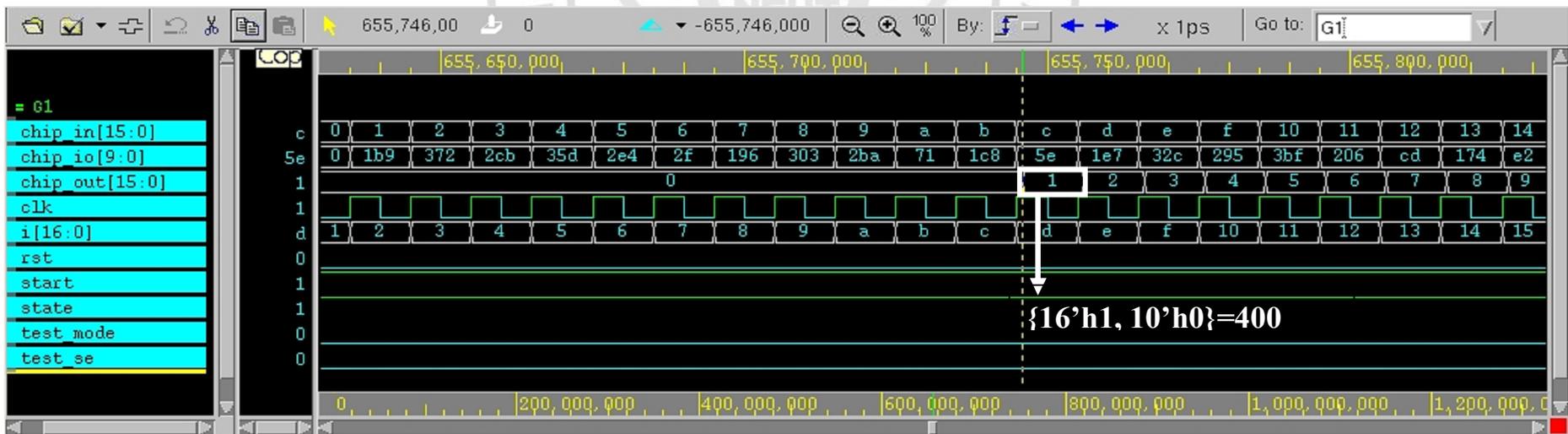


圖 4.13 解碼器合成後模擬結果

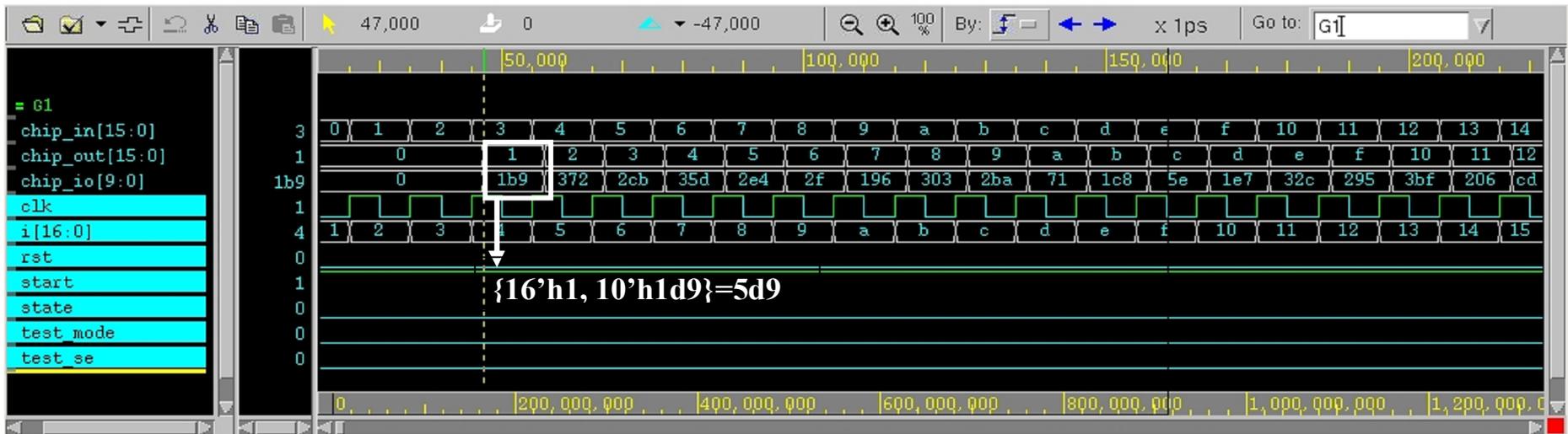


圖 4.14 編碼器佈局後模擬結果

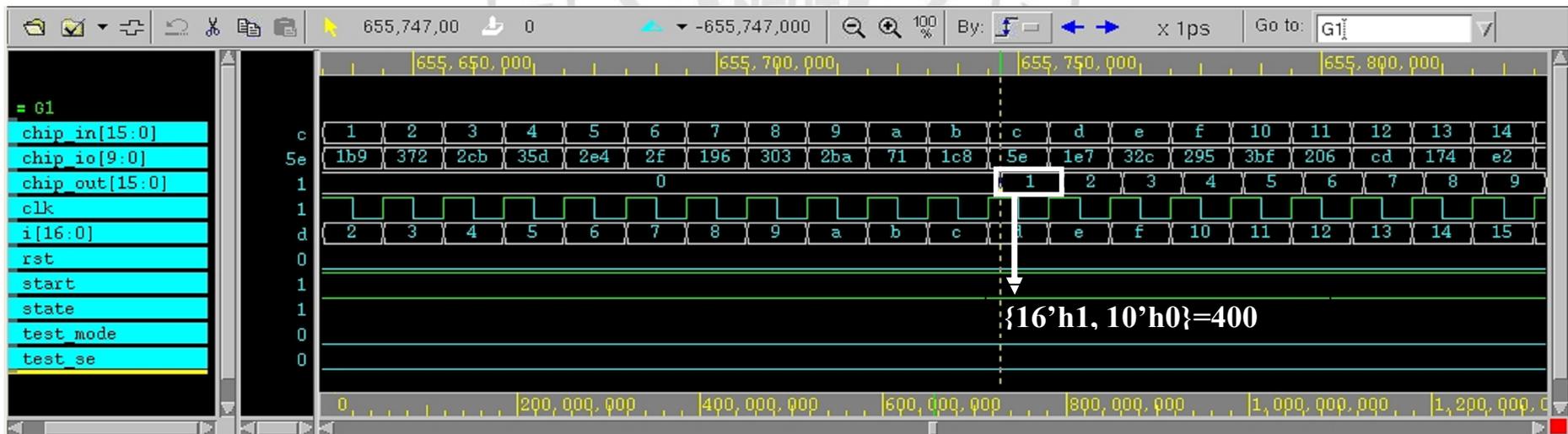


圖 4.15 解碼器佈局後模擬結果

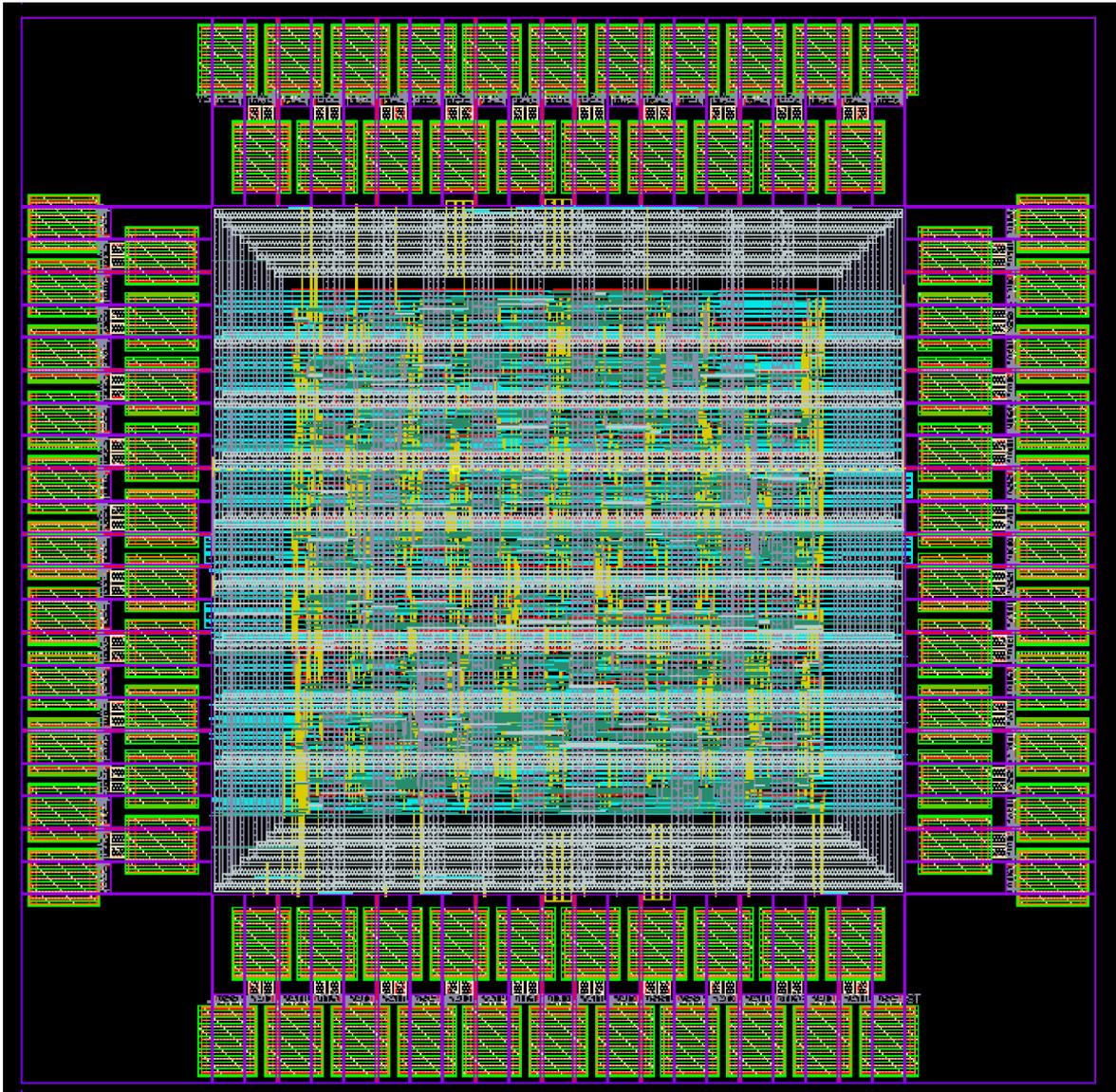


圖 4.16 晶片佈局設計圖

表 4.2 晶片預期規格表

Technology	TSMC 0.18 $\mu$ m
Power supply voltage	1.8V
Power consumption	27mW
Maximum clock frequency	100MHz
Pad number	84
Package	LCC84
CHIP area	1.048 *1.048 mm <sup>2</sup>

## 第五章 量測結果

晶片特性的量測主要是使用國家晶片中心(Chip Implementation Center,CIC)裡面所提供的 ADVANTEST V93000 PS1600 自動測試系統，該機台特色為數位及類比兼容，可用來測試混合訊號 IC 與 SOC 系統單晶片，也可以用來做 DFT 的驗證，來測試 function 的正確性，也提供了 SOC 晶片測試程式開發、SOC 晶片測試及除錯、SOC 晶片功能測試與效能分析…等等服務，如圖 5.1 所示。



圖 5.1 ADVANTEST V93000 PS1600 自動測試系統

圖 5.2 是晶片測試數位模組，上面可以看到三個放 IC 的區塊，分別是提供給 LCC68、LCC84、LCC100 去做使用，我們所使用到的是中間的 LCC84 封包。數位模組中支援的 Data Channel 數量達 512 個，其中有 128 個 Channels 的 Data Rate 可達到 1.6Gbps；另 128 個 channels 的 Data Rate 可達到 533Mbps；其餘 256 個 Channels 的 Data Rate 可達到 200Mbps。不僅如此，每個 Channel 的 Vector Memory 深度亦提高到 64M Vectors。在類比的 Instrument 共提供 4 組 Source(AWG)及 4 組 Measure(Digitizer)，其中 High Resolution 相關模組之規格皆可達 24bits；而 High Speed Source 及 Measure 模組之規格更可達 200Mpsps 及 180Mpsps。其中 Device Power Supply 更擁有 32 個 Pair，每組可支援 7V 的電壓以及總模組 48A 的電流 [28]。

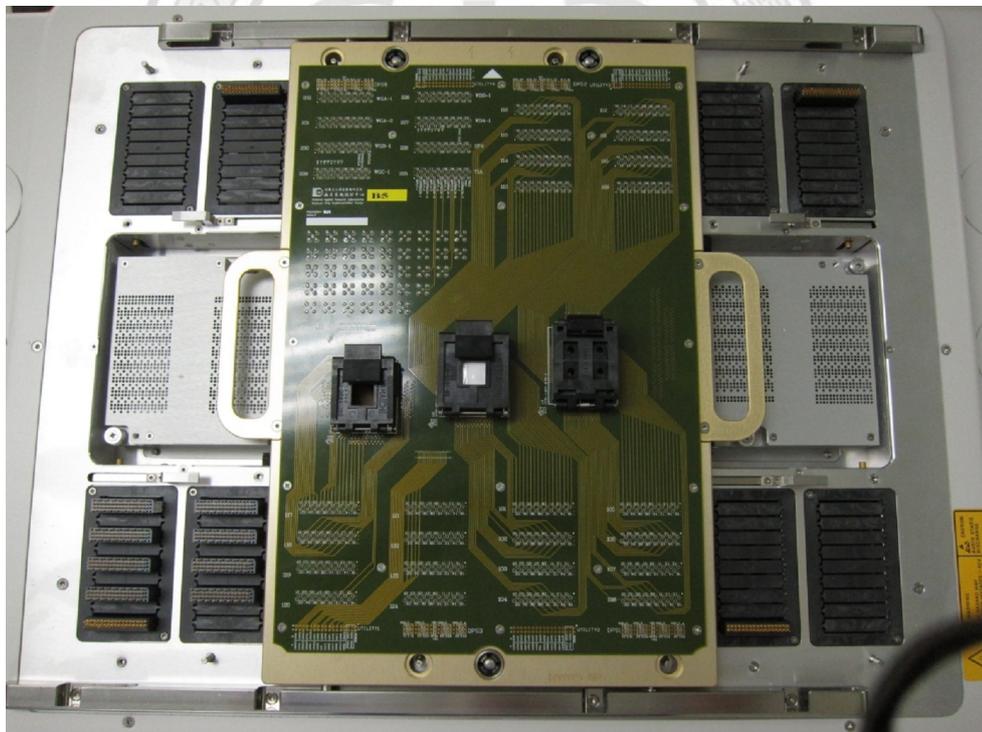


圖 5.2 晶片測試數位模組

圖 5.3 所要呈現的是輸出編碼資料的完整性，可以看到在的 2 個 clock 輸出了第一筆的 26 位元編碼資料；圖 5.4 為輸出解碼資料的完整性可以看到在的 11 個 clock 輸出了第一筆的 16 位元編碼資料。

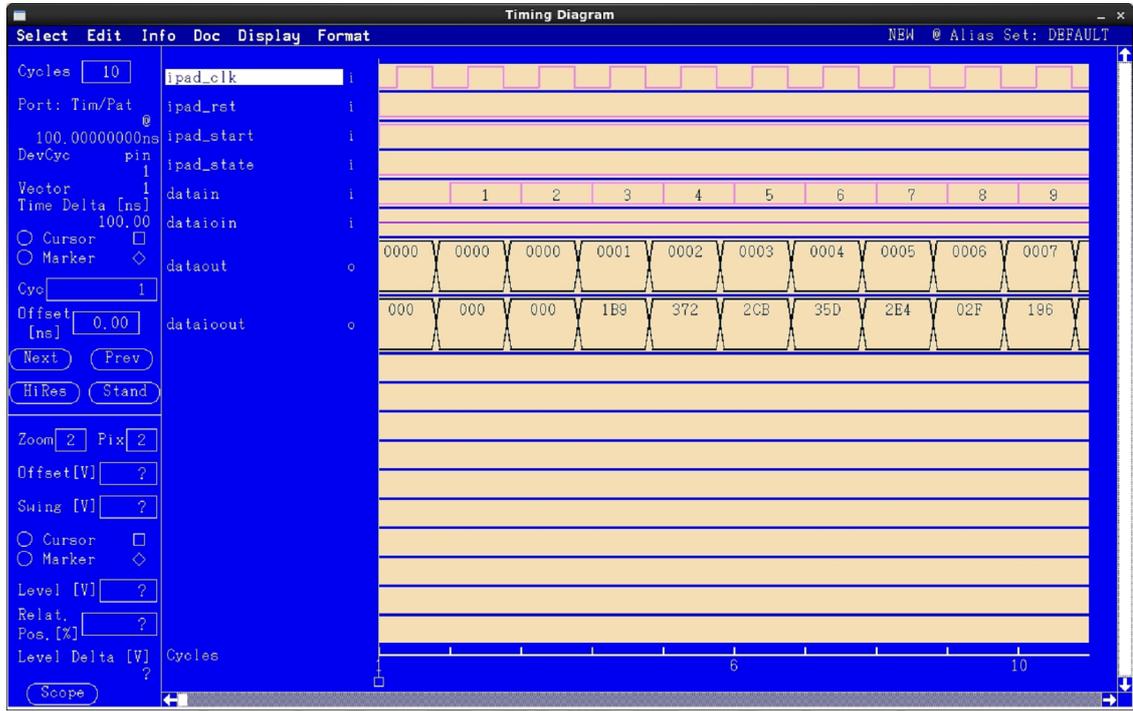


圖 5.3 編碼資料完整性

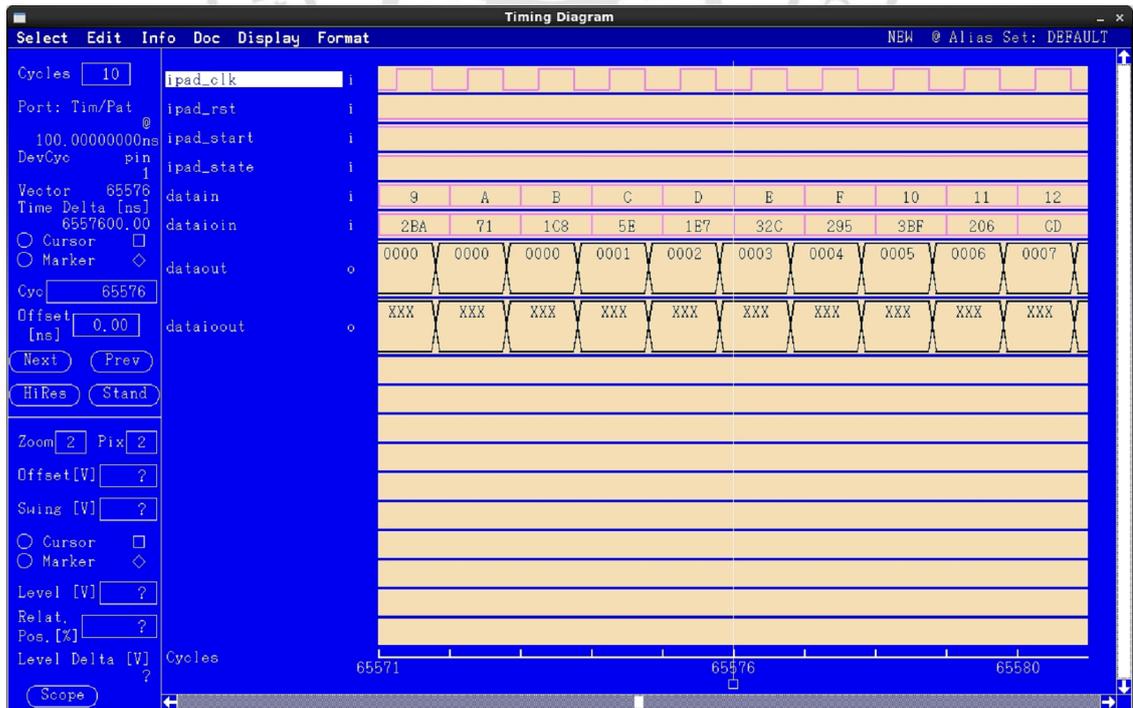


圖 5.4 解碼資料完整性

圖 5.5 是電壓-頻率比較圖，綠色部分為 pass，紅色部分為 fail，可以看到電壓在 1.8V，操作頻率可以達到 110MHz。圖 5.6 是晶片實體照片圖。

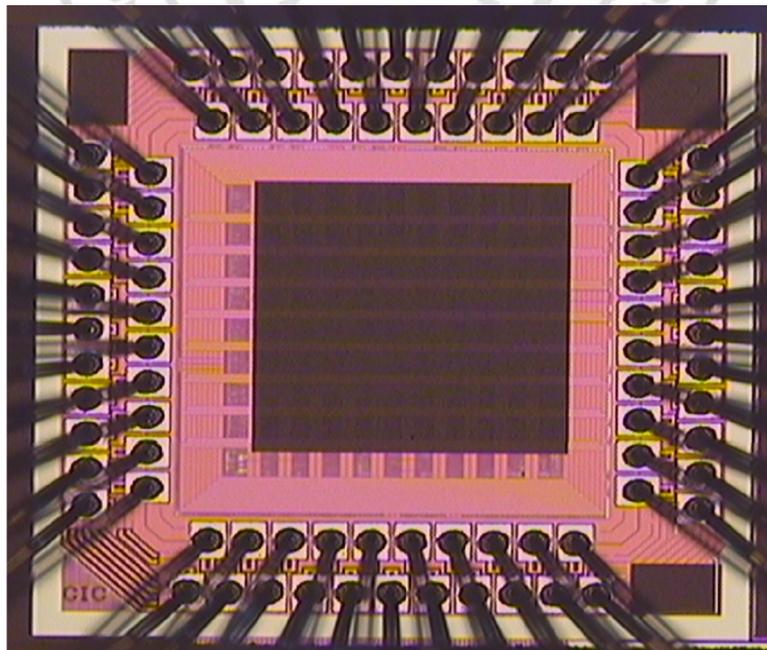
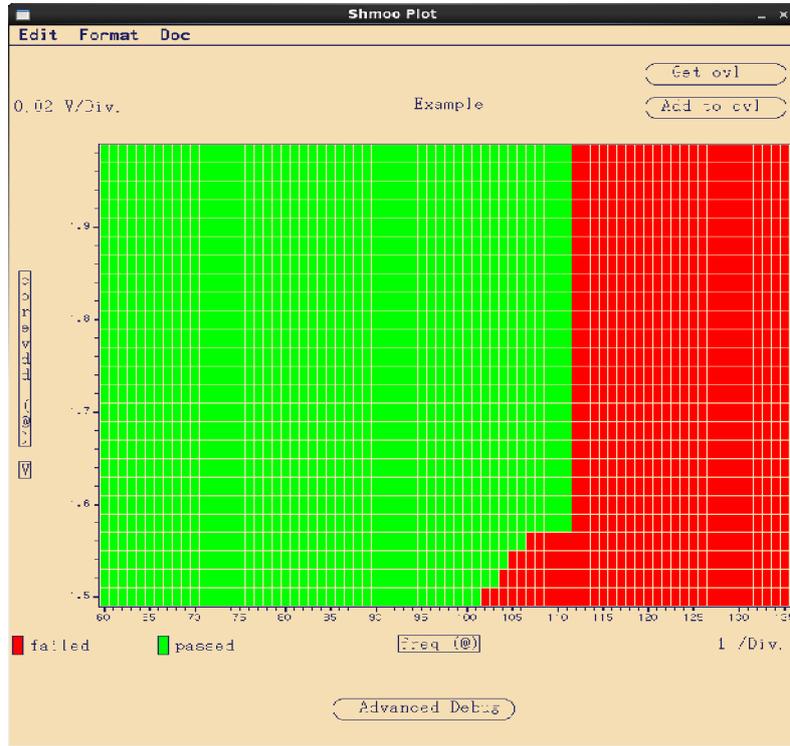


圖 5.6 晶片佈局設計圖

表 5.1 是晶片實測規格表，晶片面積為  $1.048 \times 1.048 \text{ mm}^2$ ，功率消耗則分別列出核心電路和整顆晶片在不同頻率下(100kHz、200 kHz、300 kHz、500 kHz、1MHz、50MHz、100MHz、110 MHz)的功率消耗。最高操作頻率為 110MHz，晶片功耗為 47.50mW，核心電路的功耗為 4.19mW，腳位數量是 84 隻腳，使用封包是 LCC84，供給電壓為 1.8 伏特。

表 5.1 晶片實測規格表

Technology	TSMC 0.18um
Power supply voltage	1.8V
Total power consumption	1.99mW (@ 100kHz) 2.67mW (@ 200kHz) 3.28mW (@ 300kHz) 5.41mW (@ 500kHz) 15.25mW (@ 1MHz) 24.81mW (@ 50MHz) 40.83mW (@ 100MHz) 47.50mW (@ 110MHz)
Core power consumption	0.22mW (@ 100kHz) 0.33mW (@ 200kHz) 0.42mW (@ 300kHz) 1.32mW (@ 500kHz) 1.65mW (@ 1MHz) 3.23mW (@ 50MHz) 3.63mW (@ 100MHz) 4.19mW (@ 110MHz)
Maximum clock frequency	110MHz
Pin number	84
Package	LCC84
CHIP area	$1.048 * 1.048 \text{ mm}^2$
throughput	1.76Gbps/2.86Gbps

表 5.2 列出本論文提出的架構與參考文獻比較結果，由下列的比較表可以看出，本文所提出的架構邏輯閘(Gate count)數量少於文獻[26] 75%；面積少於 88%；功率消耗少於 90%；吞吐量約為文獻[26] 3.6 倍。

表 5.2 本論文與參考文獻晶片效能比較

	This work		[26]
Technology	0.18-um		0.35-um
state	encode	decode	-
Power supply voltage	1.8V		3.3V
Pad number	84		21
Frequency	110MHz		69.8MHz/106Mhz
Gate count	32K		125K
Area	1.048*1.048 mm <sup>2</sup>		3.0*3.1 mm <sup>2</sup>
Power	47.5mW		494mW
Throughput	2.86Gbps	1.76Gbps	0.49Gbps/0.7 Gbps

## 第六章 結論

本論文針對縮短循環碼進行改良，並且考慮到硬體的複雜度、功率的消耗、面積大小與製作的成本。提出一種新的並列式編解碼架構，使用系統生成矩陣去編碼，以及系統查核矩陣與錯誤圖樣糾錯，以進行錯誤更正，並且達到高吞吐量(high-throughput)、低功耗、小面積。

循環碼的生成矩陣，主要是用來實現編碼與解碼的效能。而設計出來的新硬體架構與演算法經由 Matlab 軟體進行模擬與分析，也都能達到預期的編碼與解碼效果。在於硬體的部分，我們利用台積電公司的  $0.18\mu\text{m}$  製程來設計一個具有兩種型態的(26,16)快速編碼之循環碼編碼器，以及具突發錯誤更正之循環碼解碼器。晶片內共包含 3 萬 7 千個邏輯閘，所占的面積大小為  $1.048*1.048\text{mm}^2$  (包含 IO PAD)。實驗結果顯示此編碼器於 1.8V 下之編碼最高操作頻率可達 110MHz，而解碼器也可達到 110MHz。另外此晶片對於隨機錯誤之更正能力及突發錯誤之更正能力而言，也都具有相當好的更正能力，解碼器在位元錯誤率為  $10^{-4}$  時，其解碼增益值(coding gain)為 2.4dB。此晶片改良傳統式串列硬體電路，使其資料能夠並列輸入，讓編碼的運算時間減少了 92%，而解碼的運算時間也減少了 71%，進而增加資料傳輸的吞吐量，在最高操作頻率 110MHz 下，編碼資料吞吐量可達到 1.76Gbps，解碼電路可達到 2.86Gbps 的高吞吐量。

## 參考文獻

- [1] 李育儒, "A Simple FSK Demodulator for Wireless Communication and Design of Power and Rate Adaptation Algorithms in a Cognitive Radio Network," 國立彰化師範大學碩士論文, 中華民國九十九年七月
- [2] B. Gyselinckx, C. V. Hoof, J. Ryckaert, R. F. Yazicioglu, P. Firorini, V. Leonov, "Human++: autonomous wireless sensors for body area networks," *IEEE Custom integrated circuits conference (CICC)*, Jan. 2005.
- [3] S. V. Roy, C. Oestges, F. Horlin, P. De Doncker, "Ultra-wideband spatial correlation study for multi-sensor multi-antenna body area networks," *IET Seminar on Antennas and Propagation for Body-Centric Wireless Communications*, pp.67-70, 24-24 April 2007.
- [4] 游瑞元, "Baseband Design Techniques for Wireless Proximity Data Transmission," 國立交通大學博士論文, 中華民國九十七年七月
- [5] Hsiao-Han Ma, Jui-Yuan Yu, Tsan-Wen Chen, Chien-Ying Yu, and Chen-Yi Lee, "An OFDMA Scheme Wireless Body Area Network with Frequency Pre-Calibration," in *Proc. 2008 IEEE VLSI-DAT*, pp. 192-195, Apr. 2008.
- [6] Shuenn-Yuh Lee, Liang-Hung Wang, and Qiang Fang, "A Low Power RFID Integrated Circuits for Intelligent Healthcare Systems," *IEEE Trans. on Information Technology in Biomedicine*, 14,6, pp1387-1396, Nov. 2010.
- [7] C. E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, pp. 379-423(part 1); pp. 623-56(part 2), July 1948.
- [8] 王新梅, 肖國鎮, "糾錯碼," December 1993.
- [9] E. Prange, "Cyclic error-correcting codes in two symbols," AFCRC-TN-57, 103, Air Force Cambridge Research Center, Cambridge, Mass., Sept. 1957.
- [10] E. R. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, New York, 1968.
- [11] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed., MIT Press, Cambridge, Mass., 1972.
- [12] R. J. McEliece, "The Theory of Information and Coding", Addison-Wesley, Reading, Mass., 1977.
- [13] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes", North-Holland, Amsterdam, 1977.
- [14] C. Cheng and K. K. Parhi, "High-Speed Parallel CRC Implementation Based on Unfolding, Pipelining, and Retiming," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 53, no. 10, pp. 1017-1021, 2006.
- [15] T.-B. Pei and C. Zukowski, "High-Speed Parallel CRC Circuits in VLSI," *IEEE Transactions on Communications*, vol. 40, no. 4, pp. 653-657, Apr. 1992.
- [16] J. H. Derby, "High-Speed CRC Computation Using State-Space Transformations,"

- in IEEE International Global Telecommunications Conference, Nov. 2001, pp. 166–170.
- [17] G. Campobello, G. Patane, and M. Russo, “Parallel CRC Realization,” IEEE Transactions on Computers, vol. 52, no. 10, pp. 1312–1319, Oct. 2003.
- [18] E. Stavinov, “A practical parallel CRC generation method.” [Online]. Available: [www.OutputLogic.com](http://www.OutputLogic.com)
- [19] M. Walma, “Pipelined Cyclic Redundancy Check (CRC) Calculation,” in the Proceedings of The 16th IEEE International Conference on Computer Communications and Networks (ICCCN 2007), 2007, pp. 365–370.
- [20] C. Kennedy and A. Reyhani-Masoleh, “High-Speed Parallel CRC Circuits,” in the Proceedings of The 42nd Annual Asilomar Conference on Signals, Systems, and Computers (to appear), 2008.
- [21] J.-S. Lin, C.-K. Lee, M.-D. Shieh, and J.-H. Chen, “High-Speed CRC Design for 10 Gbps Applications,” in the Proceedings of the 2006 IEEE International Symposium on Circuits and Systems (ISCAS 2006), 2006, pp. 3177–3180.
- [22] Gilbert, E. N., “Capacity of a Burst-Noise Channel,” B.S.T.J. 39, September, 1960, pp. 1253.
- [23] Robert J. McEliece and Wayne E. Stark., “Channels with Block Interference,” IEEE Trans. On Information Theory, vol. IT-30, no. 1, pp. 44-53, Jan. 1983.
- [24] Salvatore D. Morgera and Frederic Simard., “Parameter Estimation for A Burst-Noise Channel,” IEEE International Conference on Acoustics, Speech, and Signal Processing, pp. 1701-1704, 1991.
- [25] E. O. Elliott, “Estimates of Error Rates for Codes on Burst-Noise Channels”, April 8, 1963.
- [26] 駱文華, “Chip Design of a Burst-Error-Correcting Viterbi Decoder”, June 2001.
- [27] Yu-Cheng Hung, Han-Jun Hung, “RFID Design with CRC Programmable Capability, Dual Encode Functions and Dual Modulation Outputs,” 2010 International Symposium on Next-Generation Electronics (ISNE), Nov. 2010.
- [28] 財團法人國家實驗研究室 - 國家晶片系統設計中心 Available: <http://www.cic.org.tw>

## 附錄 A. 中英對照表

中譯	英文	縮寫
人體區域網路	Body Area Network	BAN
通道	channel	
吞吐量	throughput	
資料源	source data	
錯誤更正編碼器	error correction encoder	
調變器	modulator	
解調變器	demodulator	
錯誤更正解碼器	error correction decoder	
冗餘	Redundancy	
互動式智慧型身體感測 網路晶片系統	Interactive Intelligent Body Area Network SOC	
藍芽	Bluetooth	
正交分頻多工	Orthogonal frequency-division multiplexing	OFDM
無線感測網路	ZigBee	
循環碼	Cyclic Code	
向前錯誤控制源編碼器	Forward Error Control	FEC
交錯	Inverse	
映射	Mapping	
反快速傅立葉轉換	Inverse Fast Fourier Transform	IFFT
保護區間	Guard Interval	GI
數位轉類比轉換器	Digital-to-Analog Converter	DAC
位元錯誤率	Bit Error Rate	BER
突發性錯誤	burst error	
碼字	code word	
生成多項式	generators polynomial	
徵狀	syndrome	
同位查核	Parity check	
線性	linear	
系統碼	systematic code	

廣泛性查核位元	generalized parity check bits	
縮短循環碼	Shortened cyclic code	
多路徑衰減	multipath fading	
陰影效應	shadowing	
頻道干擾	channel interference	
時變性	time-varying	
叢發性	bursty	
加成性白色高斯雜訊	Additive White Gaussian Noise	AWGN
單邊雜訊功率頻譜密度	power spectral density	
位元雜訊能量比	bit energy to noise spectral density ratio	
碼率	code rate	
突發雜訊通道模組	Burst Noise Channel Model	
馬可夫鏈	Markov Chain	
突發性錯誤修正	burst-error-correcting	
單位矩陣	identity matrix	
生成矩陣	generators matrix	
誤差圖樣	error pattern	
錯誤徵狀向量	error-syndrome vector	
查核互易多項式	reciprocal of the parity-check polynomial	
轉換	transpose	
二階相位偏移調變	Binary Phase Shift Keying	BPSK
解碼增益值	coding gain	
突發性隨機錯誤	random burst error	
硬體描述語言	Verilog hardware description language	Verilog-HDL
國家晶片設計製作中心	Chip Implementation Center	CIC
邏輯閘	Gate count	