義大研訊

Spring 2016

SEARCH & DISCOVERY

RESEARCH AT ISU & EDH

NEWS ARTICLES ACTIVITIES OPPORTUNITIES

義守大學 I-SHOU UNIVERSITY

E-DA HOSPITAL

目錄

104資訊月競賽 義大榮獲亞季軍

有資訊界奧林匹克大賽之稱的「104年資訊月資訊應用技能競賽」日前結束，義守大學土木與生態工程學系三年級張雅婷及張瑜庭同學，從全國228隊1000多人中脫穎而出，分別榮獲「工程設計技術應用競賽（AutoCAD 2014）」全國個人組亞軍及季軍，師生同感振奮。

高雄市電腦商業同業公會理事長黃水成（中）與張雅婷（右）、張瑜庭（左）合影

獲得亞軍的張雅婷說，從大一就開始接觸AutoCAD軟體，對這個比賽軟體再熟悉不過了，但參賽前還是很緊張，每天不斷地練習畫圖，經常從黑夜畫到天明。比賽規定一小時內須畫出五張圖，比速度、也比精準。她曾花2小時畫出的一張圖不夠準確，一度心生挫折，但還是不氣餒，賽前每天至少畫一張圖磨練技能，汗水終於沒有白流。

「很幸運能得到季軍!」張瑜庭謙虛地說，平時課業忙碌，靠課堂所累積的實力，以及指導老師賽前提供的書籍和題目，讓她能快速抓到重點和訣竅，而摘下銅獎。

指導老師陳崇賢表示，在系主任林國良的支持下，近2年「電腦輔助設計實習」課程輔導學生取得證照共計127張，成績相當優異。同學們課餘努力自主訓練，在AutoCAD軟體操作上技巧精熟，得獎同學也很樂意分享集訓和競賽過程，將經驗傳承給學弟妹。

AutoCAD是美國Autodesk應用電腦輔助設計技術而開發的繪圖程式軟體包，為國際上廣為流行的繪圖工具，被建築、工程與建構專業人員用來建立精確的2D 與3D 圖面。

BACK

亞太大學聯合會議首次登台
17國校長共商創業人才培育

31屆亞洲暨太平洋大學聯合會議(The Association of Universities of Asia and the Pacific Conference，簡稱AUAP)，21-23日在高雄義大皇家飯店登場，這是AUAP首次於台灣舉辦，有17個國家地區、近60所大專校院及相關教育機構校長及主管，約500人出席盛會，共同探討亞太地區高等教育如何與產業結合，以培育創業人才等議題。

亞太地區校長聯合會議21日在義大皇家酒店的「戰鼓」表演聲中揭開序幕

今年AUAP主題「創新與創業：亞太地區高等教育快速發展的角色」，AUAP主席陳肖純博士(大陸鄭州西亞斯國際學院創辦人)、主辦單位義守大學校長蕭介夫博士(AUAP理事)、教育部國際及兩岸教育司長楊敏玲博士，以及美國、英國、日本、南韓、紐西蘭、印度及伊朗等國貴賓皆分享寶貴的經驗。

義大校長蕭介夫表示，今年AUAP主題「創新與創業」，與義大集團辦學背景吻合。義大在25年前，由擁有全球第三大不?鋼廠的義联集團董事長林義守先生所創辦，現有近18,000名學生，近50國、2,000名境外生就讀，姊妹校超過415所，2015年9月入榜《英國泰晤士報高等教育特刊》全球最佳大學排行榜前800大，其中「產學合作」項目排名世界第344名，是台灣最具潛力又優質的國際化綜合大學。

義守大學校長蕭介夫主持亞太地區校長聯合會議

同樣是企業興學有成的泰國卜蜂集團總裁蔡緒峰先生，以「高等教育創新與創業」為題，分享泰國7-11透過鼓勵員工進修，改造企業體質，創造出「人才流失率從15%降至3%，商品失竊率從2.5%降至0.3%」的驚人成果。

義大國際及兩岸事務處長林許淑謙博士，分享義大在「創造力與創新挑戰」的治校經驗說，25多年前，南台灣人才難尋，創辦人林義守先生為回饋鄉里、善盡社會責任，以企業興辦義大。「目前擁有400多家產學家族，義联集團多年來提供豐富的產學、實習資源與就業機會，學子在義大就讀看得到未來，真正落實『學用合一』與『創業型大學』的目標」。

亞太地區校長聯合會議21日在義大皇家酒店登場，與會貴賓大合照

21日下午還有大學校長國際聯盟(IAUP)主席Neal F. King博士，主講「如何成為一所創業型大學」；行政院科技部國家實驗研究院科技政策研究與資訊中心主任莊裕澤，亦分享「台灣創新與創業公私部門合作夥伴關係」。

AUAP成立於1995年，為連結亞太地區各大學共同推動優質高等教育環境，並促進區域和平與國際交流的組織，為聯合國教科文組織(UNESCO)所認可，現有23國、近240所大學會員，包括澳洲格里菲斯大學、香港大學、伊朗首都德黑蘭大學、澳門大學、印尼大學及大陸西安大學等著名高教學府，台灣則包含義大，共有6所大學加入。

BACK

全國私校第一
義守大學成立原住民族學院

義守大學校長蕭介夫宣布，2月1日將成立原住民族學院，這是全國私立大學的第一、也是西部地區的唯一。校方每年將祭出近千萬元獎勵原住民學生就讀，並媒合義大世界提供實習及打工機會，讓經濟弱勢的原住民學生能夠安心就學。

義守大學積極培養原住民學生的國際視野及部落文化素養

各校面臨嚴峻的少子化衝擊，但義守大學本於照顧偏遠弱勢學生的初衷，不僅沒有縮編原住民專班的規模，反而更積極投入原住民族高等教育。蕭介夫校長指出，義守大學在民國101年成立原住民族發展中心，開始招收原住民專班的學生，

目前原住民專班已有觀光餐旅、傳播設計、護理及長期照護4個班，每年招收100多名來自全臺灣包括花東及蘭嶼等偏遠地區的原住民學生，全校共有600多名原住民同學，是國內原住民學生最多的大學。

義守大學是繼國立東華大學之後，第二個成立原住民族學院的大學，為照顧來自偏鄉的學生，除每年編列800多萬的住宿及助學金提供原民生4年免費住宿之外，為慶祝原住民族學院的成立，將加碼提供新台幣100萬元設立「大武山獎助學金」，鼓勵原住民族學院同學努力向學，同時安排學生校內工讀，以及媒合義大世界提供實習及打工機會，讓原住民族學院學生不用擔心學費及生活費沒有著落。

義守大學原住民專班學生在去年校慶時表演傳統部落歌舞

未來原住民族學院將統合觀光餐旅、傳播設計、護理及長期照護4個專班，並設計符合當前原住民社會發展需要的課程，同時開設更多原住民族文化與族語類科目，鼓勵學生認同並積極學習自己的傳統文化，成為未來部落發展與文化振興的厚實力量。

BACK

引擎啟動供電器
義大學生創新專題競賽奪冠

你曾因為忘了關掉汽車大燈，導致整輛車無法啟動嗎？義守大學電機工程學系學生研發「引擎啟動供電器」，可以發出電壓過低信號，提醒駕駛人注意；這項作品勇奪創新專題競賽金牌，並已提出專利申請。

引擎啟動供電器（指標處）

義守大學創新專題競賽今年邁入第五屆，共有85隊403人次參賽，戰況空前。電機系在吳榮慶、張恩誌兩位老師指

導下，林志明、蕭志洋、黨浩凡、曾俊傑及林彥佐5名同學以「生活智慧王」自封，五個金頭腦激盪研發出「引擎啟動供電器」，可提醒車主檢查電池壽命，避免無法發動上路。

引擎啟動供電器設計製作團隊，左起為蕭志洋、林志明、吳榮慶老師、曾俊傑、黨浩凡

吳榮慶老師說，他曾因大燈沒關導致車子無法啟動，加上很多車主在車上加裝行車記錄器、GPS、防盜器或超速警示器等電子設備，造成電池不勘負荷，這時候如果有個耗電量極低，且能偵測汽車是否能發動的裝置，就能避免上述問題發生。

師生研發的「引擎啟動供電器」就像個黑盒子，可以插在點煙座上，在引擎起動後才供電給外接裝置，保護電池不被外接電子設備耗光；並具備電池壽命警示功能，當汽車電池的電

壓過低時，引擎啟動供電器就不會亮紅燈，可提醒駕駛人電池電量已不足，是該檢查電池壽命的時候了。該設備在待機時，具有靜態電流極低的功能，長時間不開車情況下該設備也不會把電池的電耗光。。

林志明同學表示，剛開始為測試哪種方法才可行，修改了十幾種的設計方式，最後摸索出這套汽車電池的保護系統，「很高興能得到金牌，希望未來能商品化」。

產學智財營運總中心智權技轉組長黃克穠表示，創新專題競賽目的在激發學生的創新想法，並透過此競賽實現創作，協助學生申請專利，參加國際級發明展，讓外界能看見學生的研發能量。

BACK

國際師生力拚認證
義守大學再創顛峰

成功的背後，是一群人默默流著汗水。義守大學申請AACSB認證，動員不計其數的國內外師生及校友，經過5年的努力，終於取得這項全球商管教育品質的桂冠。擁有百年歷史的AACSB，是全球最權威的商學院認證、也是管理教育領域最具影響力的認證機構。通過認證，對位在南台灣邊陲、教育資源遠不如北部的義守大學而言，是一條漫長而艱困的道路。但義守大學不僅做到了，更為創校25年來再創新猷，憑藉著是一股向上提升的力量。

為挑戰這項高難度的證認，義大管理、觀光餐旅與國際三個學院總動員，在近二千個日子裡，歷經一遍又一遍的內部審核、評估和調整，師生都融入「持續精進」的氛圍中。三度獲得傑出教學獎的會計系老師莊素增，組成團隊設計「會計學共識測驗題庫」，能準確測出學生的會計基礎知識，並培養學生會計倫理素養；她所組成的報稅服務隊，服務高雄在地居民長達19年，每年服務逾2萬人次，更讓AACSB審查委員稱讚連連。

不只是本國師生全力拚搏，外籍師生也從剛開始的觀望

到後來的認同，進而全心投入。澳洲籍的國際觀光餐旅系老師歐彼得(Peter O' Brian)，協助檢查上百頁的英文報告書，讓它更有「英文味」；同樣來自澳洲的國際企業學系老師湯小美(Paula Tomsett)，亦主動蒐集文獻，減少認證過程的摸索期。

通過認證最直接的受益者是學生。首屆管理學院管理碩士班國際組(IMBA)畢業的曾湘樺，是前高雄縣大樹鄉長曾英志的女兒。回想起2009年進修期間，她說：「感受到一股向上的校園氛圍，自己也提升了經營與分析能力」。畢業後與退休老爸共同創業，將大樹區特產玉荷包釀酒後加入香腸中，讓大樹名產四季都飄香，自己也成為「百萬型農」。行銷、財務與業務一把罩的她，還把當地名產推向國際舞台。如今嘗到認證成果的喜悅，就像她的酒釀玉荷包般甘甜。

首屆 IMBA 畢業生曾湘樺，是前高雄縣大樹鄉長曾英志女兒。將大樹區特產玉荷包釀酒後加入香腸中，成為「百萬型農」

來自廣東深圳、曾在泰國某大學就讀飯店管理陸生張子廉，曾在普吉島五星級飯店實習，因慕名義联集團企業辦學，集團旗下又有皇家與天悅兩家飯店，實習與出路寬廣，選擇再來台就讀義守大學企業管理研究所。擁有開創夢想飯店的他說：「看著校方全心投入AACSB認證工作，心中著實感動，這趟跨海求學沒有白來。」

來自廣東陸生張子廉，慕名義聯集團企業辦學，又有皇家與天悅兩家飯店，選擇再來台就讀義守大學企業管理研究所

目前全球僅有不到5%的商管學院取得AACSB認證，三個學院同時通過更是絕無僅有，代表義守大學長期以來追求教學卓越和改善學習環境的深耕，獲得高度肯定，也為南台灣學子開啟邁向國際的康莊大道。

BACK

失智症問題行為的非藥物改善措施之實證建議

李慧琦[1]、李逸[2]、林佑樺[3]、劉憶慧[4]

義守大學 護理系 講師[1]
義守大學 護理系 助理教授[2]
義守大學 護理系 教授[3,4]

摘要

失智症患者有逐年增加的趨勢，而90%失智症患者會出現問題行為，造成照顧者憂鬱與嚴重的負擔。本文主要依據問題行為定義，利用文獻查證方式探討統合分析研究中非藥物改善措施對失智症患者問題行為的成效。透過系統性搜尋發表於AgeLine、CINAHL、Cochrane library、MEDLINE、PsycARTICLES、PsycINFO及PubMed資料庫，逐一閱讀全文後共8篇符合本文納入條件。結果發現感官刺激活動、合併性音樂治療、情境模擬療法、功能性分析及個案管理是能有效善失智症問題行為，然而缺乏具體時間建議及收尋文獻中納入非隨機對照試驗均為本文限制，此研究成果期望能對臨床護理照護及未來研究有所貢獻。

關鍵字：失智症、問題行為、非藥物改善措施、統合分析

前言

全球失智症盛行率及發生率有逐年增加的趨勢，西元2010年人口數已高達三千六百萬人，預估西元2030年會增加為目前的兩倍，西元2050年會增加為三倍[1]。依據統計，約90%失智症患者會出現問題行為(problem behavior) [2]，問題行為被視為最易造成照顧者負擔、憂鬱及精神疾病[3]，因此問題行為常被認為是失智症患者

照顧上最大挑戰之一[4]。本文主要是以文獻查證方式探討統合分析研究有關失智症患者問題行為非藥物措施的成效，以期對臨床護理措施有實證性建議。

背景

一、問題行為的定義與臨床表徵

人類行為(human behavior) 是指個人的身體活動(physical actions)，此身體活動反應個人對環境刺激或內在驅力的感知能力，並建構在過去學習經驗、個人特質、性別、文化，並合併精神疾病、身體功能、及許多合併因素[5]。問題行為可能是神經-解剖或神經-化學的不正常，此缺損造成患者對環境刺激及回憶過去學習經驗的正確感知能力受到干擾，並損害患者的因應機制、抽象思考能力及處理外在環境改變的執行能力[5]。

問題行為又稱為破壞行為(disruptive behaviors)、干擾行(disturbing behaviors)、行為問題(behavioral problems)、攻擊行為(aggressive behaviors)焦躁不安(restless)[6, 7] 。Cohen-Mansfield & Billig(1986)[8] 將躁動行為(agitated behaviors)定義為「不適當的語言、聲音或動作等；這些行為不被觀察者判斷是直接由躁動病人的需要或混亂(confusion)造成」。Kolanowski (1995)[6] 概念分析將破壞行為(disruptive behaviors)分為下列五個概念：(1)心理性肌肉運動激動行為(Aggressive Psychomotor Behavior)：指會傷害或抵抗別人的行為；(2)心理性肌肉運動非激動行為(Nonaggressive Psychomotor Behavior)：引起別人注意的重複行為，但此行為不會傷害他人；(3)言語攻擊行為(Verbally Aggressive Behavior)：攻擊別人的言語行為；(4)消極行為(Passive Behavior)：冷淡並缺乏與外界互動；(5)功能喪失行為(Functionally Impaired Behavior)：喪失自我照顧的功能且行為表現造成其他人困擾。

藥物治療常用來減緩失智症問題行為，但常有惡化認知功能、嗜睡、尿道感染、錐體外症候群(extra-pyramidal symptoms)及不正常的步態等副作用[9]。許多研究致力於失智症患者問題行為非藥物措施，但其結果多樣不一致。證據金字塔(evidence pyramid)以統合分析(meta-analysis)為實證依據最高等級[10]，本篇主要是以

文獻查證方式去深入瞭解有關失智症患者問題行為非藥物措施統合分析研究，以期對護理措施有實證性建議。

非藥物改善措施之實證建議

一、文獻查證方法

本文之文獻查證主要資料庫主要為AgeLine、CINAHL、Cochrane library、MEDLINE、PsycARTICLES、PsycINFO 及 PubMed。資料庫查詢時間為2015年2月13日到2015年2月23日。關鍵字為problem behavior、disruptive behaviors、disturbing behaviors、aggressive behaviors、restless、meta-analysis、dementia。文獻之納入條件為：（1）統合分析文章(meta- analysis)；（2）非藥物介入措施；（3）失智症患者；（4）測量變項為問題行為。文獻之排除條件為：（1）系統性文獻回顧；（2）僅一篇文章納入統合分析；（3）藥物介入措施；（4）質性研究統整分析。

總共查詢到77篇文章，經Endnote軟體刪除重複性的研究(n = 15)後，共62篇，檢視摘要排除文章(n = 48)後共14篇，檢視全文後共刪除6篇，其理由為：質性統合分析(Qualitative meta-synthesis)(n = 1)；研究變項為非問題行為(n = 1)；問題行為研究數量太少或異質性太高僅只有做文獻分析(n = 4)，故共8篇文獻納入本文分析(圖一)。

八篇文獻中，有5篇納入統合分析研究均為隨機對照試驗（Randomized Controlled Trials, RCTs）[11-14]，有3篇納入統合分析研究包含非隨機對照試驗[15-17]。非藥物措施有亮光療法(light therapy)、職能治療(occupational therapy)(含感官刺激活動(sensory stimulation)、音樂治療(music Therapy)、功能性分析(functional analysis)、情境模擬療法(simulated presence therapy)及個案管理(case management)(表一)。

二、非藥物措施成效

統合成效依非藥物措施的結果如列所述：

感官刺激活動主要是藉由燈光效應、觸覺物體表面、冥想音樂及放鬆精油的氣味等方法，給予視覺、聽覺、觸覺、味覺、及嗅覺刺激以增進正向行為並減少不合適行為[18]。共3篇統合分析文獻，有兩篇為顯著性效果[12, 13]，一篇未達顯著性效果[11]。Kim等人[12]統合分析研究6篇職能治療研究(4篇以感官刺激活動為

主， 2篇環境改變活動(environmental modification) 為主，只有感官刺激活動有顯著性改善問題行為，活動次數為每次約30分鐘，每週2~3次，持續4~10週，只有有一篇執行6次活動。Kong等人[13]統合分析14篇非藥物治療研究，發現只有感官介入措施有顯著性效果，此感官介入措施包含：芳香療法(aromatherapy)、熱浴(thermal bath)、平靜音樂(calming music)、及手部按摩(hand massage)，持續時間約至少為2個月，然而此篇文獻發現有異質性較高 (I2 = 68.2%)。

但如果只有單一亮光療法卻沒有達顯著性改善，Forbes等人[11]統合分析4篇亮光療法，結果發現問題行為沒有顯著性改善，其統合分析大部分研究中的燈光治療為每天1~2小時，持續時間為10天到 1星期的2500 到 10,000 lux亮光。

在音樂治療面，總共有2篇統合分析文獻[15, 16]，均顯示音樂治療能有效改善問題行為。Koger等人[15] 統合分析21篇比較性研究文章，並將社會/情緒、認知及行為測量項目一起分析發現，音樂治療是有顯著性改善。Ueda, Suzukamo, Sato 及Izumi (2013) [16] 統合文獻11篇隨機對照實驗及非隨機對照實驗研究發現音樂治療能改善失智症患者的行為，如：激動不安(agitation)、冷淡(apathy)、興高采烈(elation) 和易怒(irritability)，這些研究中音樂治療介入措施大多為合併性音樂治療，如：唱歌、玩樂器、和聽音樂，每天約30分鐘，一週約2-3天，共約10週，其中只有一篇研究執行期間為一週。然而此2篇文獻在異質性分析發現有較高的情形(分別為homogeneity test: $p < .05$及$I2 > 50\%$)。

其他對行為治療有顯著性改善的如情境模擬療法、功能性分析、個案管理。Zetteler (2008)[17]統合分析四篇非隨機對照試驗，發現情境模擬療法對問題行為有顯著性效果，此情境模擬療法主要是藉由撥放錄音帶或錄影帶給失智個案聆聽或觀看，其內容包個案過去的正向生活經驗，及家人和朋友的經驗分享。Moniz Cook等人[14]統合分析發現行為分析治療能有效改善失智個案問題行為的頻率，但無法改善問題行為發生率及嚴重度，此行為分析治療主要是指醫護人員或家庭照顧者先了解個案問題行為的前因後果，以給予適當照護措施。Reilly等人[19]統合分析研究則發現個社區性個案管理在第18個月有顯著效果，但在第

4、6、12個月未達顯著，個案管理的措施包括：鼓勵個案自我安排照顧及確認提供適當的服務。

結論與討論

本文主要是利用文獻查證方式去分析非藥物改善措施的成效，在8篇統合分析文獻中，感官刺激活動、合併性音樂治療、情境模擬療法、功能性分析及個案管理是能有效善失智症問題行為，但若只有亮光療法卻沒有顯著性改善。而在這些措施中，需要長時間執行才能達到顯著性效果，如：感官刺激活動時間約為1~2月、音樂治療約10週、個案管理約18個月。

本文限制為，在這些文獻設計發現，仍有少部分文獻為統合分析非隨機對照試驗，如音樂治療均為分析非隨機對照試驗。如果統合分析採用缺乏嚴謹度的隨機對照試驗研究設計或使用非隨機對照試驗研究，可能會因為其他變項而干擾因果推理的強度[20]。再者，可能是缺乏非藥物改善措施對失智症行為的相關研究，在查詢文獻中缺乏統合分析次群組分析(subgroup- analysis)，因此在執行措施頻率及期間無法給予具體建議，且可能因為不同收案對象的特質、不同的評量工具及研究場所造成異質性過高。

在未來建議方面，比起藥物措施，非藥物措施有較少的危險性[13, 21]，但藥物與非藥物措施成效相互比較、及非藥物改善措施的成本、副作用及照顧者是否容易執行，本文均未作深入研究，期待未來研究能針對上述做深入分析以提供失智患者問題行為更具體的改善措施。

參考文獻

[1]World Health Organization(2012), Dementia: a public health priority, http://www.who.int/mental_health/publications/dementia_report_2012/en/.

[2]J.K.K.M. Fung, H.W.H. Tsang, and R.C.K. Chung (2012), A systematic review of the use of aromatherapy in treatment of behavioral problems in dementia, *Geriatrics & Gerontology International*, vol. 12, no. 3, pp. 372-382; DOI 10.1111/j.1447-0594.2012.00849.x.

[3]J. van der Lee, T.J. Bakker, H.J. Duivenvoorden, and R.M. Droes

(2014), Multivariate models of subjective caregiver burden in dementia: a systematic review, *Ageing Res Rev*, vol. 15, , pp. 76-93; DOI 10.1016/j.arr.2014.03.003.

[4]C.K. Lai, J.H. Yeung, V. Mok, and I. Chi (2009), Special care units for dementia individuals with behavioural problems, *The Cochrane database of systematic reviews*, no. 4, pp. Cd006470; DOI 10.1002/14651858.CD006470.pub2.

[5]D.A. Smith (2008), Behavioral problems and symptoms in dementia, *Journal of the American Medical Directors Association*, vol. 9, no. 9, pp. 622-625.

[6] A.M. Kolanowski (1995), Disturbing behaviors in demented elders: a concept synthesis, *Archives of Psychiatric Nursing*, vol. 9, no. 4, pp. 188-194.

[7]高潔純(2004)，機構失智長者的問題行為，*長期照護雜誌*，8(2)，251-261。.

[8] J. Cohen-Mansfield and N. Billig (1986), Agitated behaviors in the elderly. I. A conceptual review, *J Am Geriatr Soc*, vol. 34, no. 10, pp. 711-721.

[9] L.S. Schneider, K. Dagerman, and P.S. Insel (2006), Efficacy and adverse effects of atypical antipsychotics for dementia: meta-analysis of randomized, placebo-controlled trials, *The American journal of geriatric psychiatry : official journal of the American Association for Geriatric Psychiatry*, vol. 14, no. 3, pp. 191-210; DOI 10.1097/01.JGP.0000200589.01396.6d.

[10]D.F. Polit, and C.T. Beck (2011), Nursing research: Generating and assessing evidence for nursing practice, 9th Edition., Lippincott Williams & Wilkins.

[11]D. Forbes, C.M. Blake, E.J. Thiessen, S. Peacock, and P. Hawranik (2014), Light therapy for improving cognition, activities of daily living, sleep, challenging behaviour, and psychiatric disturbances in dementia, *The Cochrane database of systematic reviews*, vol. 2, pp. Cd003946; DOI 10.1002/14651858.CD003946.pub4.

[12]S. Y. Kim, E. Y. Yoo, M. Y. Jung,

S. H. Park, and J. H. Park (2012), A systematic review of the effects of occupational therapy for persons with dementia: A meta-analysis of randomized controlled trials, *NeuroRehabilitation*, vol. 31, no. 2, pp. 107-115.

[13]E.H. Kong, L.K. Evans, and J.P. Guevara (2009), Nonpharmacological intervention for agitation in dementia: a systematic review and meta-analysis, *Aging & mental health*, vol. 13, no. 4, pp. 512-520; DOI 10.1080/13607860902774394.

[14]E.D. Moniz Cook, K. Swift, I. James, R. Malouf, M. De Vugt, and F. Verhey (2012), Functional analysis-based interventions for challenging behaviour in dementia, *The Cochrane database of systematic reviews*, vol. 2, pp. Cd006929; DOI 10.1002/14651858.CD006929.pub2.

[15]S.M. Koger, K. Chapin, and M. Brotons (1999), Is music therapy an effective intervention for dementia? A meta-analytic review of literature, *Journal of Music Therapy*, vol. 36, no. 1, pp. 2-15.

[16]T. Ueda, Y. Suzukamo, M. Sato, and S.-I. Izumi (2013), Effects of music therapy on behavioral and psychological symptoms of dementia: A systematic review and meta-analysis, *Ageing Research Reviews*, vol. 12, no. 2, pp. 628-641; DOI 10.1016/j.arr.2013.02.003.

[17]J. Zetteler (2008), Effectiveness of simulated presence therapy for individuals with dementia: a systematic review and meta-analysis, *Aging and Mental Health*, vol. 12, no. 6, pp. 779-785.

[18]J.C. Chung, C.K. Lai, P.M. Chung, and H.P. French (2002), Snoezelen for dementia, *The Cochrane database of systematic reviews*, no. 4, pp. Cd003152; DOI 10.1002/14651858.cd003152.

[19]S. Reilly, C. Miranda-Castillo, R. Malouf, J. Hoe, S. Toot, D. Challis, and M. Orrell (2015), Case management approaches to home support for people with dementia, *The Cochrane database of systematic reviews*, vol. 1, pp. Cd008345; DOI

10.1002/14651858.CD008345.pub2.

[20]H. Cooper, L.V. Hedges, and J.C. Valentine (2009), The handbook of research synthesis and meta-analysis, Russell Sage Foundation.

[21]G. Livingston, K. Johnston, C. Katona, J. Paton, and C.G. Lyketsos (2005), Systematic review of psychological approaches to the management of neuropsychiatric symptoms of dementia, *The American journal of psychiatry*, vol. 162, no. 11, pp. 1996-2021; DOI 10.1176/appi.ajp.162.11.1996.

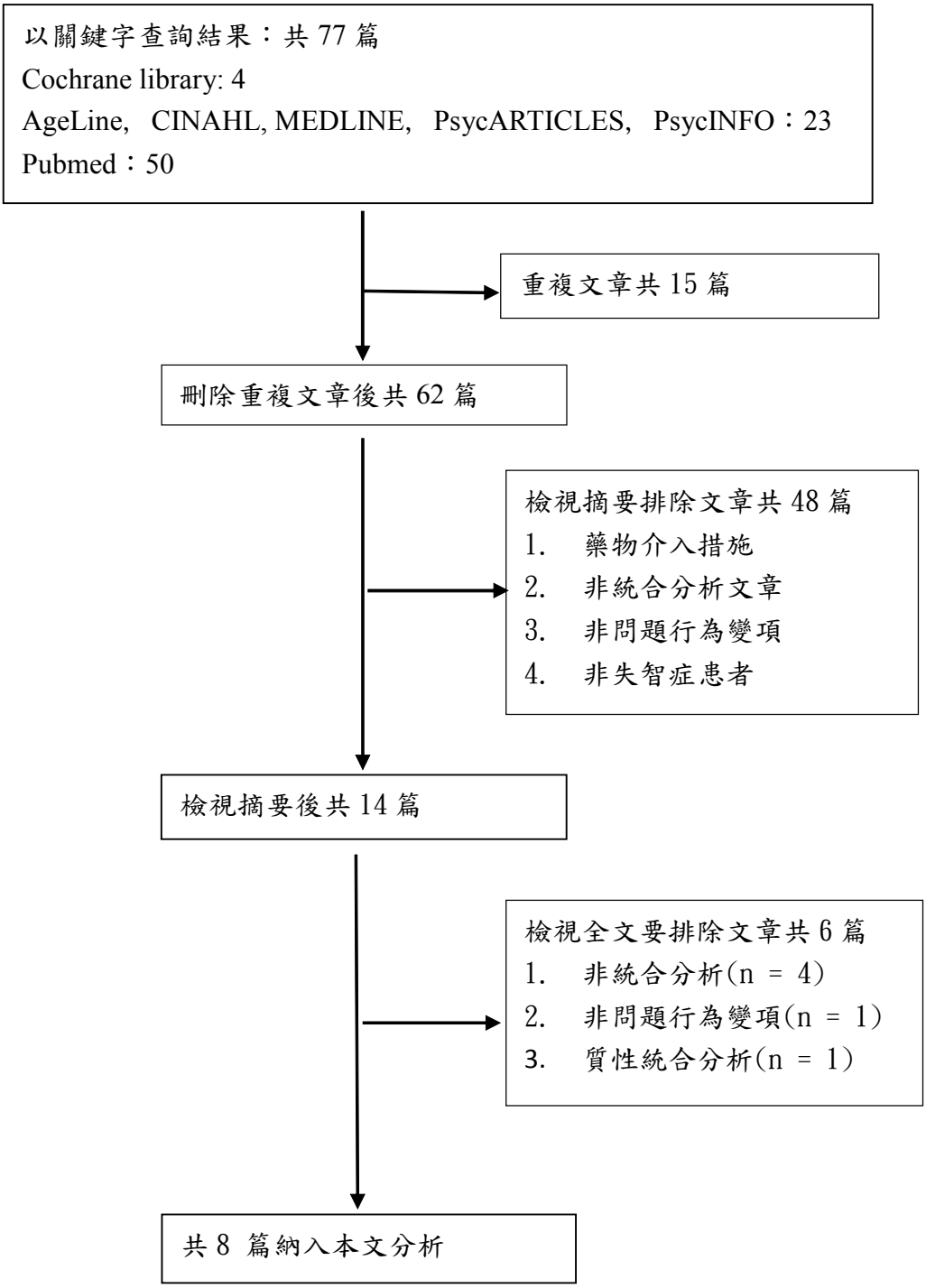
表一：文獻彙整

作者 / 年代	分析文章數量 / 研究方法	研究對象 / 地點	介入措施	測量工具	結果
1.Forbes, Blake, Thiessen, Peacock, & Hawranik (2014)[11]	4 / RCTs	失智症 / 護理之家	亮光療法 (light therapy).	ABRS	p > .05
2.Kim, Yoo, Jung, Park, & Park(2012)[12]	感官刺激活動 :4 環境改變活動 :2 / RCTs	失智症	職能治療： 感官刺激活動 (sensory stimulation)； 環境改變活動 (environmental modification)	MBPC RMBPC BMD BRS	感官刺激活動：p < .05 環境改變活動：p > .05

作者 / 年代	分析文章數量 / 研究方法	研究對象 / 地點	介入措施	測量工具	結果
3.Koger, Chapin, & Brotons(1999) [15]	21 / non-RCTs	失智症	音樂治療 (music therapy)	社會 / 情緒、認知及行為	社會 / 情緒、認知及行為： $p > .05$ (homogeneity test: Q (20)= 51.485, p= .0001)
4. Kong, Evans, & Guevara(2009) [13]	14 / RCTs	失智症 / 護理之家及社區	非藥物介入措施 (nonpharmacological interventions)	CMAI ABMI Behave-AD ABID PAS DBS	感官介入措施：$p < .05$ (Test for heterogeneity: Chi–square= 6.28, df = 2 (p =.04,I^2 = 68.2%) 社會接觸 (social contact)、活動 (activities), 環境改變活動 (environmental modification)、照顧者訓練 (caregiver training)、合併治療 (combination therapy)、行為治療 (behavioral therapy)： $p > .05$
5.Moniz Cook 等人 (2012)[14]	發生率：4 頻率：10 嚴重度：2 / RCTs	失智症 / 社區或相關機構	功能性分析 (functional analysis)	RMBPC CMAI NPI	頻率：$p < .05$ 發生率、嚴重度：$p > .05$
6.Reilly 等人 (2015)[19]	4 個月：2 6 個月：4 10-12 個月：5 18 個月：2 /RCTs	失智症 / 社區	個案管理 (case management)	NPI RMBPC	第 4、6、12 月：$p > .05$ 第 18 月：$p < .05$

作者 / 年代	分析文章數量 / 研究方法	研究對象 / 地點	介入措施	測量工具	結果
7.Ueda, Suzukamo, Sato, & Izumi(2013) [16]	11 /RCTs and non-RCTs	失智症	音樂治療 (music therapy)	CMAI Inventory Behavioral Symptomatology in Alzheimer's Disease scale NPI NPI-Q; BOP scale:	$p < .05$ (heterogeneity: Tau2 = 0.17；Chi2 = 23.63; df = 10 (p = .009); I2 = 58%)
8.Zetteler (2008) [17]	4 / non-RCTs	失智症	情境模擬療法 (simulated presence therapy)	DBRS CMAI HRS	$p < .05$

備　註：ABID = The Agitated Behavior Inventory for Dementia; ABMI = The Agitation Behavior Mapping Instrument; ABRS = Agitated Behavior Rating Scale; Behave-AD = The Behavioral Pathology in Alzheimer's Disease Rating Scale; BMD = Behavior and Mood Disturbance Scale; BOP scale = Beoordelingsschaal voor Oudere Patienten; BRS = Behavior Rating Scale; CMAI = Cohen-Mansfiedl Agitated Inventory; DBRS = Disruptive Behaviour Rating Scale; HRS = Haycox Rating Scale; MBPC = Memory and Behavior Problems Checklist; NPI = Neuropsychiatric Inventory; NPI-Q = Neuropsychiatric Inventory-Brief Questionnaire Form; PAS = The Pittsburgh Agitation Scale; RCTs = Randomized Controlled Trials; RMBPC = Revised Memory and Problem Behavior Checklist



圖一：文獻篩選流程圖

BACK

改良高糾錯率之Reed-Solomon Code解碼技術於二維條碼

陳延華[1] 林威任[2]

義守大學 資訊工程學系 副教授[1]
義守大學 資訊工程學系 學生[2]

摘要

隨著智慧型手機的普及，二維條碼變得更加便利取得資訊，二維條碼(QR code)對於資料除錯主要使用Reed-Solomon code (RS碼)，有限體GF(28)規格下進行編碼與糾錯，由於二維條碼容錯方式可分成L, M, Q, H等四種容錯率，而本論文主要針對QR code高容錯率的規格Q (容錯率25%) 與H (容錯率30%) 進行解碼速度改良，由於容錯率越高在糾錯解碼計算過程中就越耗時，尤其在計算症狀子 (Syndrome) 過程中更需要大量運算時間，本論文透過查表法與改良霍納法則 (Horner's Rule) 加速二維條碼在糾錯解碼時的執行速度，使得在解碼更具即時性。實驗方法則使用開放原始碼的二維條碼解碼程式，且在Android系統的行動裝置測試改良二維條碼解碼程式解碼效率，最後分析出方法使用C++語言或是使用JAVA語言執行效率的問題。

關鍵字: 症狀子、霍納法、二維條碼、RS碼

前言

目前很多商品都以二維條碼方式[1-2]儲存資訊，如幾乎每天都會取得的電子發票或是路邊常見的文宣海報，都會附上二維條碼讓使用者能取得更多的資訊，而二維條碼中以Reed-Solomon code[3-6]編碼儲存資訊，此種編碼的特性在解碼過程必須使用不少時間，其中一個重要環節為計算症狀子，而本論文研究的目標為探討如

何減少症狀子計算量的方法。現在的二維條碼解碼器在計算症狀子的方法上面主要是使用霍納法，以二維條碼規格所使用之GF(28)，如果使用查表法減少運算必須建立32種排列組合的表格(大小為256*256*32)，而本研究所使用的方法為建立8種排列組合的表(256*256*8)，雖然能使用較少的記憶體空間，但缺點是必須執行比較多次的查表與加法運算量。利用ZXing (zebra crossing) 所提供二維條碼解碼器原始碼[2]，植入改良計算症狀子的程式碼進行討論，ZXing所提供二維條碼開放原始碼，計算症狀子的方法以主要利用霍納法，而一般霍納法在計算症狀子所需要有限體乘法[7-9]數量與加法數量，會跟隨資料長度n-1增加，所以在實驗步驟與分析中會以不同n長度的方式進行解碼性能測試，由於ZXing提供的原始碼大多以物件 (Class) 型態撰寫，為了比較的公平性，本論文所測試的數據為將其改成非物件的方式撰寫。

研究方法

Reed-Solomon Code的症狀子計算必須將$\alpha^0 \sim \alpha^{2t-1}$的根代入接收訊息多項式$R(x)$，如果只使用傳統的霍納法，不同的根帶入$R(x)$之間的運算並無關聯，因此提出一個新的計算症狀子的方式，讓計算症狀子之間，只需要透過補差量就能獲得計算結果，達成減少乘法運量的方法，並且配合查表法的部分，先行運算部分結果建立表單資料，進而提升症狀子的計算速度。然而，所提出的方法有其缺點，當要補症狀子補差量時必須使用大量記憶體，由於事先透過事先計算儲存的查表數值，在執行程式時，可以透過查表法減低CPU運算量，因此方法相對就比使用傳統霍納法的解碼速度快很多，由於提出方法是實現在Android系統的行動裝置，而且使用JAVA語言撰寫執行，是否具備有C語言撰寫執行的相同效能，將在實驗結果進行說明。實驗過程使用C++與Java兩種語言撰寫症狀子計算的程式，並且比較執行的速度差異比較，最後改為NDK方式執行程式進行手機實體測試，將在實驗步驟與分析中詳細介紹。

研究方法

症狀子使用傳統霍納法

症狀子的計算一般作法為使用霍納法，根據不同的t將$\alpha^0 \sim \alpha^{2t-1}$的根代入多項式計算得到$S_0 \sim S_{2t-1}$。以(7, 3, 4)

RS碼，有限體GF(2^3)為例：

令 $R(x)=\alpha^6x^6+\alpha^5x^5+\alpha^4x^4+\alpha^3x^3+\alpha^2x^2+\alpha^1x^1+\alpha^0$

症狀子：$S_0=R(\alpha^0)$ 、 $S_1=R(\alpha^1)$ 、 $S_2=R(\alpha^2)$ 、 $S_3=R(\alpha^3)$

將R(x)以霍納法表示：

$$R(x)=(((((\alpha^6x+\alpha^5)x+\alpha^4)x+\alpha^3)x+\alpha^2)x+\alpha^1)x+\alpha^0 \quad (1)$$

依據公式(1)，症狀子$S_0\sim S_3$ ：

$$S_0=R(\alpha^0)=(((((\alpha^6\alpha^0+\alpha^5)\alpha^0+\alpha^4)\alpha^0+\alpha^3)\alpha^0+\alpha^2)\alpha^0+\alpha^1)\alpha^0+\alpha^0$$

$$S_1=R(\alpha^1)=(((((\alpha^6\alpha^1+\alpha^5)\alpha^1+\alpha^4)\alpha^1+\alpha^3)\alpha^1+\alpha^2)\alpha^1+\alpha^1)\alpha^1+\alpha^0$$

$$S_2=R(\alpha^2)=(((((\alpha^6\alpha^2+\alpha^5)\alpha^2+\alpha^4)\alpha^2+\alpha^3)\alpha^2+\alpha^2)\alpha^2+\alpha^1)\alpha^2+\alpha^0$$

$$S_3=R(\alpha^3)=(((((\alpha^6\alpha^3+\alpha^5)\alpha^3+\alpha^4)\alpha^3+\alpha^3)\alpha^3+\alpha^2)\alpha^3+\alpha^1)\alpha^3+\alpha^0$$

透過此方法計算這些症狀子需要6次乘法與6次加法的運算時間，共有四組症狀子，所以需要24次乘法與24次加法的運算時間，或以查表方式需要24次查表，建表大小為2^3*2^3*4 (其中4，為RS碼2t的值，當t=2)。

症狀子使用改良式霍納法

論文使用的方法將對R(x)多項式三項為一組(稱之為一個black)並且配合霍納法則：

$$R(x)=(\alpha^6x^2+\alpha^5x+\alpha^4)x^3+(\alpha^3x^2+\alpha^2x+\alpha^1)x+\alpha^0 \quad (2)$$

令：

$B_0(x)=\alpha^0$ 、 $B_1(x)=(\alpha^3x^2+\alpha^2x+\alpha^1)$ 、

$B_2(x)=(\alpha^6x^2+\alpha^5x+\alpha^4)$ 。

$L_2(x)=(\alpha^6x^2+\alpha^5x)$ 、 $L_1=(\alpha^3x^2+\alpha^2x)$ ，

$L_{20}=L_2(\alpha^0)$ 、 $L_{21}=L_2(\alpha^1)$ 、 $L_{22}=L_2(\alpha^2)$ 、

$L_{10}=L_1(\alpha^0)$ 、 $L_{11}=L_1(\alpha^1)$ 、 $L_{12}=L_1(\alpha^2)$ 。

依照本論文的方法，除了S_0，其餘症狀子均以補差量方式計算，差量函式：

$$\Delta_i(x)=L_{i2}x_2+L_{i1}x_1+L_{i0}x_0 \quad (3)$$

其中$x=x_2x_1x_0$ ，$x_i\in\{0,1\}$ 。R(x)的症狀子$S_0\sim S_4$ 改成下式：

$$S_0=R(\alpha^0)=(L_2(\alpha^0)+\alpha^4)x^3+(L_1(\alpha^0)+\alpha^1)x^1+\alpha^0$$
$$=(B_2(\alpha^0)x^3+B_1(\alpha^0)x^1+B_0(\alpha^0)$$

$$S_1=(B_2(\alpha^0)+\Delta_2(\alpha^0+\alpha^1)x^3+B_1(\alpha^0)+\Delta_1(\alpha^0+\alpha^1)x^1+B_0(a^0)$$

$$S_2=(B_2(\alpha^1)+L_2(\alpha^1+\alpha^2)x^3+B_1(\alpha^1)+L_1(\alpha^1+\alpha^2)x^1+B_0(\alpha^1)$$

$$S_3=(B_2(\alpha^2)+L_2(\alpha^2+\alpha^3)x^3+B_1(\alpha^2)+L_1(\alpha^2+\alpha^3)x^1+B_0(\alpha^2)$$

由上面範例所示，提出的症狀子計算方法需要建立大小為2^3*2^3*3 (3為$GF(2^3)$的3次方)與一個$(\alpha^i)^3$ 的表格大小為7，每個症狀子需要2個乘法，所以共8個乘法，加法為40次。然而二維條碼使用是使用$GF(2^8)$實作RS碼，如以霍納法需要建立表格的方程式為$f(x)=\alpha_ix+\alpha_j$ 其中i、j皆從0~254，須建立32張表格，即$x=\alpha^0\sim\alpha^3$ 。而本論文所需建立之方程式為$f(x)=\alpha_ix^2+\alpha_jx$ 其中i、j同樣皆從

0~254，但只須建立8張表單，為 $x=\alpha^0 \sim \alpha^7$ ，另一張$(\alpha^i)^3$的表格大小為254，所以所提出的方法具節省建表的優勢。

實驗步驟與分析

實作症狀子計算程式過程

ZXing所提供的二維條碼解碼器原始碼，其症狀子計算程式如圖一所示紅色方框內程式碼，但這部分程式又呼叫另一個Function為圖二的程式碼，在圖三中才是使用霍納法做症狀子計算。論文所提出的方法實作出症狀子的計算程式，將撰寫的程式碼直接放入ZXing的檔案中如圖二所示，程式碼並沒有分成多個Function或Class方式撰寫，所以直接代換，放入新的演算法程式如圖三。最後進行實際二維條碼解碼性能測試。

未查表與查表症狀子計算結果分析

二維條碼解碼器是使用有限體$GF(2^8)$的RS碼，設定長度n並非固定，而是根據除錯能力增減長度，因此症狀子的計算可分成三部分說明:

第一部份：長度為n的RS碼可分為$\lfloor n/3 \rfloor$個區塊，而每個區塊需要一次乘法、一次加法與兩次查表(一次為查區塊的結果、另一次為x^3查表運算)。

第二部份：$S_1 \sim S_{2t-1}$同樣有$\lfloor n/3 \rfloor$個區塊，而主要計算方式為補差量，每個區塊運算需要九次的加法，八次的查表與一次的乘法運算，但實際實現時可以減少一次加法與一次查表。

第三部份：剩餘不足一組的符號數為n除3的餘數(表示為n%3)，本論文直接以霍納法的方式計算，且$S_0 \sim S_{2t-1}$的情況相同，所以需要$2t \times (n\%3)$個乘法與加法。

綜合以上三部份，所有需要的查表次數、加法數量、乘法數量如下：

查表次數：$2*\lfloor n/3 \rfloor + 8*\lfloor n/3 \rfloor *(2t-1)$

加法次數：$\lfloor n/3 \rfloor + (n\%3) + \left(9*\lfloor n/3 \rfloor + (n\%3)\right)*(2t-1)$

乘法次數：$\left(\lfloor n/3 \rfloor + (n\%3)\right) \times 2t$

分析結果，理論上整體可以省下2/3的乘法數量、加法大約多3倍 (隨著n變大，乘法數量與加法數量變多)，另一個代價為必須大量查表，數量大約與加法次數相同，實際測試數據如圖四與圖五。根據圖四與圖五的數據顯示出使用JAVA語言撰寫，不利於查表法。因此改以NDK的方式實作於二維條碼解碼器中，以改善JAVA使用查表法運算不佳的問題，實驗結果如圖六所示。

結論

論文所使用的方法能否減少症

狀子計算時間，跟查表速度有極大關係，而所改良的二維條碼解碼器主要是針對Android系統，使用Java語言，在高糾錯率下利用Java撰寫查表法，不能有效提升速度反而會降低速度。因此如果在Android系統下要使用查表法則必須透過NDK呼叫C語言的方式，才能有效提升症狀子的計算速度，根據圖六所顯示的實驗數據可以得知，比傳統霍納法減少約36%的運算時間。

參考文獻

[1]QR code規格書，ISO_IEC_18004_2006

[2]二維條碼解碼器：https://github.com/zxing/zxing

[3]I. S. Reed and G. Solomon (1960), Polynomial codes over certain finite fields, *Journal of the Society of industrial and Applied Mathematics*, vol. 8. pp. 300-304.

[4] S. B. Wicker (1994), Error Control systems for Digital Communication and Storage, Englewood Cliffs, *N.J.: Prentice-Hall*.

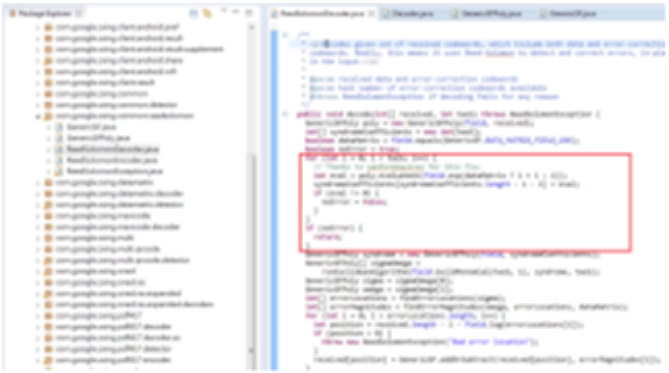
[5] Wicker and Bhargava (1994), Reed-Solomon Codes and Their Applications, *IEEE Press*.

[6] T.R.N. RAO and E. Fujiwara (1989), Error--Control Coding for Computer Systems, *Prentice-Hall*.

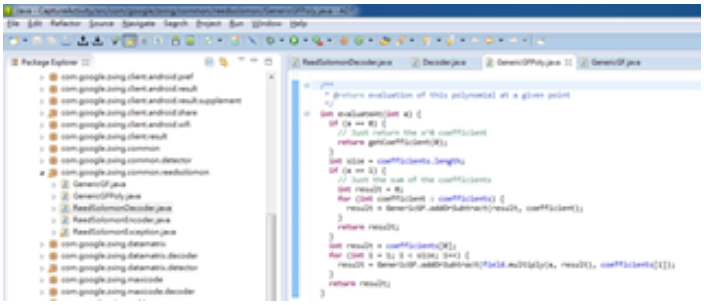
[7] P. K. Meher (2009), Systolic and Non-Systolic Scalable Modular Designs of Finite Field Multipliers for Reed–Solomon Codec, *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 17, pp. 747-757.

[8] J. L. Imaña, J. M. Sánchez, and F. Tirado (2006), Bit-parallel finite field multipliers for irreducible trinomials, *IEEE Trans. Computers*, vol. 55, no.5, pp. 520–533.

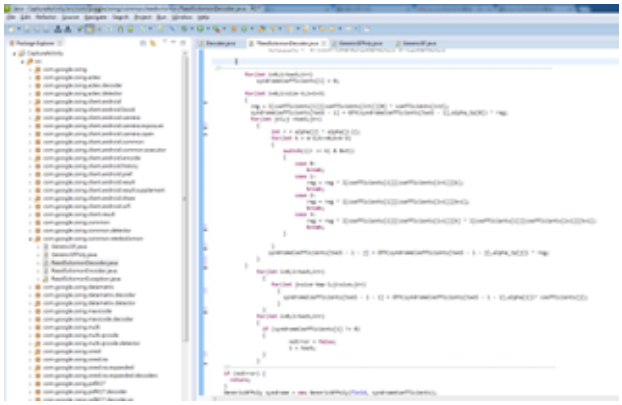
[9] H. Wu (2006), Low complexity bit-parallel multiplier for a class of finite fields, *in Proc. Int. Conf. Commun., Circuits Syst*., vol. 4, pp. 565–568.



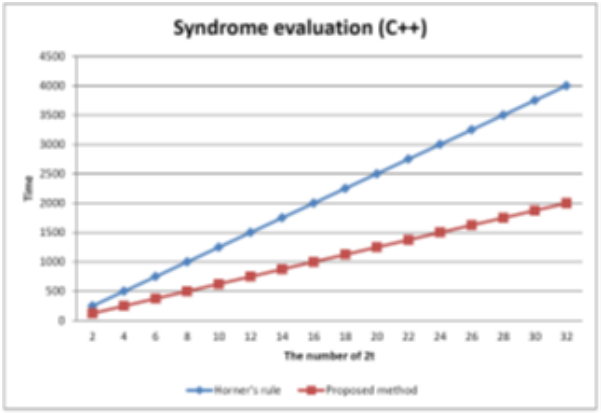
圖一、ZXing 程式計算症狀子接口



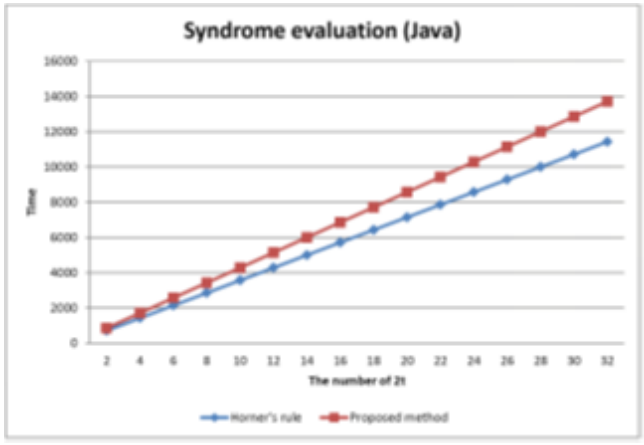
圖二、使用霍納法做症狀子計算



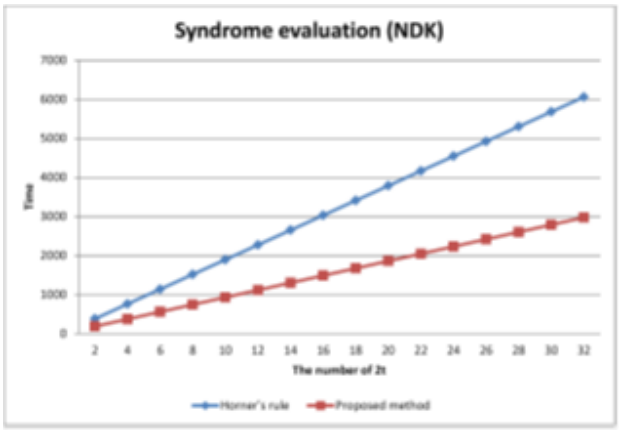
圖三、程式碼實作於二維條碼解碼器



圖四、利用 C++ 程式計算症狀子時間分析



圖五、使用 Java 程式計算症狀子時間分析



圖六、使用 NDK 症狀子計算時間分析

BACK

研究添加鋁元素於CM247LC鎳基超合金之高溫氧化行為

顏嘉緯[1]、簡騰瑞[1]、郭振明[2]

義守大學　材料科學與工程學系[1]
義守大學　機械與自動化工程學系[2]

摘要

本研究採合金設計之觀點，以CM247LC鎳基超合金作為材料基底，透過不同比例的鋁元素微量添加(0.5、1、1.5、2wt.%)，經由真空熔煉及單方向凝固鑄造法製成並進行高溫氧化試驗。此次高溫恆溫氧化實驗設計時數為100、200、300hr，並利用掃描式電子顯微鏡(SEM)、能量色散X-射線光譜(EDS)進行顯微組織觀察及成分分析。實驗顯示，CM247LC超合金在添加鋁元素後，促進γ'相的析出，使γ'相體積百分率也隨著增大，提高基材的強度，並促進形成連續氧化鋁層，以提高耐氧化性。

關鍵字：單方向凝固、鎳基超合金、鋁元素添加、高溫氧化

前言

當今社會科技日新月異，人們所使用的產品更是不斷的汰舊換新，倘若追溯到人類工業史上最大的躍進不免就要提到十八世紀在英格蘭的工業革命，當時改良後的蒸汽機，引發出動力機器能代替人力的概念，而在1930s發明出氣渦輪引擎，隨著科技進步渦輪引擎的應用及需求量大幅提升，對渦輪引擎的規格及適用環境的可耐溫度也隨之升高，而這些渦輪引擎葉片也大量運用在航太業包括海、陸、民航、軍用上。進而衍生出的問題在於現今提倡環保概念，但在所謂的航太業運用超合金製造出的引擎、渦輪葉片也好都是需要常常汰舊換新的大零件，所以對於航太業上的超合

金材料選擇格外的重要，而為配合在應用環境下，擁有耐高溫、抗腐蝕、抗潛變等高溫機械性質的鎳基超合金便獲得重用，當然不只原材料本身的性質，在不同領域、環境下的運用，原料的來源、等級、主要的組成元素、含有害相含量、不純物質以及微量元素、熔煉的方法、抗腐蝕性與機械性質等等都是需要在每次的開發應用中審慎的分析及核准，可看出合金種類的強度發展及高溫強度不斷進步中[1-4]。

超合金分類主要分為三大類型，鎳基(Nickel-base)超合金、鐵基(Iron-base)超合金、鈷基(Cobalt-base)超合金，超合金材料是從1940s二次大戰時期大量運用在航空渦輪葉片及發動機中，而三種合金中鎳基應用上最為廣泛，以鎳(Ni)為主要基材元素[5]，包含至少10種以上的合金元素(Ti、Al、Cr 等)所組成，屬於耐高溫材料。在高溫環境下擁有良好的高溫強度以及韌性、抗潛變性能、熱疲勞、抗高溫腐蝕以及氧化、高延展性及銲接性能優異，易於加工鍛造。

CM247LC是一種含碳量低的鑄造鎳基超合金，主要是在1978年後期將Mar-M247鎳基超合金進行不同的化學元素改質，改良最多在於碳(C)大幅降低，主要是為了改善Mar-M247會產生過多的碳化物，這也是CM247LC(Low Carbon)低碳的命名意義，不同於前身Mar-M247，CM247LC在鑄造過程中晶界不會產生裂紋，結合改進的硬質合金微觀結構和延展性，專為單方向凝固鑄造(DS)渦輪葉片和刀片使用[6-9]，CM-247LC超合金與Mar-M247超合金組成差異表如表1[10]。

超合金中，主要以Al和Ti元素的添加使得γ'析出高體積百分率，其中Al成本較便宜也較容易取得，也是選用Al的原因之一。本研究以合金設計的觀點，透過添加微量Al元素的改變，探討CM-247LC鎳基超合金其顯微組織與在高溫氧化後氧化層生成比較。

實驗原理與方法

本實驗選用CM247LC鎳基超合金作為材料基底，添加不同比例的鋁元素，經由真空熔煉感應爐(VIM)分別與0.5wt.%、1wt.%、1.5wt.%、2wt.%的鋁重新熔煉，成分表如表2，鑄錠後再經由單方向凝固鑄造(DS)形成單方向凝固試棒，並進行熱處理，熱處理分為三階段，熱處理程序如圖1，熱處理完成後利用氬氣進行冷卻。試片經切

割、研磨至5mm進行高溫恆溫氧化實驗，高溫恆溫氧化實驗原理主要是模擬陸上發動機渦輪葉片在高溫環境工作下的情形，氧化實驗溫度訂為1000°C，氧化時間分別為100hr、200hr、300hr。實驗後利用掃描式電子顯微鏡SEM及EDS對高溫氧化後CM247LC鎳基超合金添加不同比例鋁元素以及不同氧化時數的微組織觀察及成分分析。

結果與討論

3.1 CM247LC 添加不同鋁元素熔煉後微觀組織觀察

本實驗利用真空感應熔解爐(VIM)熔煉和單方向凝固(DS)鑄造CM-247LC鎳基超合金添加0.5wt.%、1wt.%、1.5wt.%、2wt. Al，可從顯微組織中觀察原料CM247LC與添加鋁元素後γ'相大小、形狀皆有明顯差異如圖2，但在鑄造過後之試片析出強化相γ'相晶粒排列較不整齊，以及有產生其餘γ-γ'共晶相和基地相析出的MC型碳化物的疑慮，這些組織結構對材料的機械性質及高溫性質皆為不利之影響，而為了改善此問題，後續的熱處理就顯得相當關鍵重要。

3.2 熱處理後微觀組織觀察

圖3是經過固溶熱處理與時效熱處理後的顯微組織結構，比較在經過熱處理後γ'相排列整齊、大小、形狀較一致，相對熱處理前皆有明顯的改善，而且未熱處理的顯微結構中的粗大γ'相已溶至基地相而呈現小立方體的型態，同時熱處理也消除了γ-γ'共晶相。這些效果表示了我們設定的熱處理參數對於CM247LC鎳基超合金單方向凝固鑄造之試棒，能改善並獲得優異的顯微組織結構。

在熱處理後，CM247LC原料其γ'相經過計算後體積分率約為69%，而添加0.5wt.%、1wt.%、1.5wt.%、2wt.%Al之合金較大則分別約為72%、78%、85%、88%，可以發現隨著Al的添加，合金之γ'強化相的體積分率有明顯提升，添加Al元素目的之一就在於鎳(Ni)與鋁(Al)反應後能析出γ'強化相(NiAl)，因此本實驗希望增加Al的含量能藉此提高γ'相在顯微組織中的體積百分率，阻擋差排滑移現象提升機械強度，其中可以發現在添加0.5wt.%之Al元素時，合金擁有大小一致且有序排列的γ'相。

3.2 熱處理後微觀組織觀察

依序將五種試片(CM247LC原料及添加四種不同比例鋁元素試片)分別進行三組不同時間的高溫恆溫氧化測試，總共15組試片再分為添加不同比例鋁元素試片觀察以及同比例鋁元素不同氧化時間試片觀察。

從試片剖面圖4來看，不論氧化時間的長短，γ' precipitate-free zone(PFZ)層會依添加Al元素的比例逐漸變窄，以氧化時間200hr來看，CM247LC原料至添加2wt.%Al元素之試片，PFZ層由5μm變窄至2μm，就目前看來PFZ層厚度變窄能提高連續氧化層的生成增強抗氧化性。

圖5再以不同角度加以觀察，以未添加Al元素試片、添加0.5wt.%Al試片和添加2wt.%Al試片進行比較，隨著氧化時間拉長CM247LC表面的氧化層也隨之增加，且有一不連續的Al_2O_3層生成在氧化層及連續Al_2O_3保護層之間，由此可知，當CM247LC逐漸發生氧化時，其生成的Al_2O_3保護層不足以保護基地相，因此發生內氧化的現象較有添加Al的試片嚴重。但在添加2wt.%Al元素的試片中看到連續的氧化層並無添加0.5wt.%Al試片來得好，反而產生不連續的氧化層導致材料受到內氧化的影響。

結論

本研究以合金設計的觀點，選用CM247LC鎳基超合金為材料基礎，透過添加微量Al元素的改變(0.5wt.%、1wt.%、1.5wt.%、2wt.%)，來探討高溫氧化後對微觀組織的影響與變化，得到以下之結論：

1.CM247LC超合金試片熱處理前後，微觀組織、γ'強化相有明顯的差異，原本存在的γ-γ'共晶相，MC型碳化物皆能有效消除，γ'相排列也較整齊、大小、形狀一致。

2.在SEM微觀觀察中，隨著Al元素的添加在CM-247LC中，有明顯的促進γ'強化相析出，提高體積分率，其中在添加0.5wt.%之Al元素時，擁有大小一致且有序排列的γ'相。

3.微量添加Al元素在CM247LC鎳基超合金，不僅可以提升超合金中的Al活性，並促進Al2O3氧化層在高溫下快速生成連續緻密的保護層，能有效提升高溫抗氧化性能。

參考文獻

[1] M. J. Donachie and S. J. Donachie (2002), in: "*Superalloys A Technical Guide 2nd Edition*", ASM International, USA.

[2] F. R. N. Nabarro and H. L (1995). de Villiers, in: "*The Physics of Creep 1st Edition*", CRC Press, British.

[3] C. T. Sims and W. C. Hangel (1972), in: "*The Superalloys*", John Wiley & Sons, Inc., New York.

[4] C. T. Sims, N. S. Stoloff, and W. C. Hangel (1987), in: "*Superalloys II*", John Wiley & Sons, Inc., New York.

[5] C. T. Sims, N. S. Stoloff, and W. C. Hangel, *Superalloy II*, John Wiley & Sons, Inc., New York, pp.4-8.

[6] A. sato, Y.L. Chiu, and R.C. Reed (2011), Oxidation of nickel-based single-crystal superalloys for industrial gas turbine applications, *Acta Mater*. vol. 59 , pp. 225-240.

[7] I.V.S. Yashwanth, I. Gurrappa, and H. Murakami (2011), Oxidation behavior of a newly developed superalloy, *J. Surf. Eng. Mater. Adv. Technol.* vol. 1, p. 130.

[8] M. Bensch, A. Sato, N. Warnken, E. Affeldt, R.C. Reed, and U. Glatzel (2012), Modelling of high temperature oxidation of alumina-forming single-crystal nickel-base superalloys, *Acta Mater.* vol. 60, pp. 5468-5480.

[9] D. C. Madeleine (1997), *The Microstructure of Superalloys 1st Edition*, CRC press, USA,.

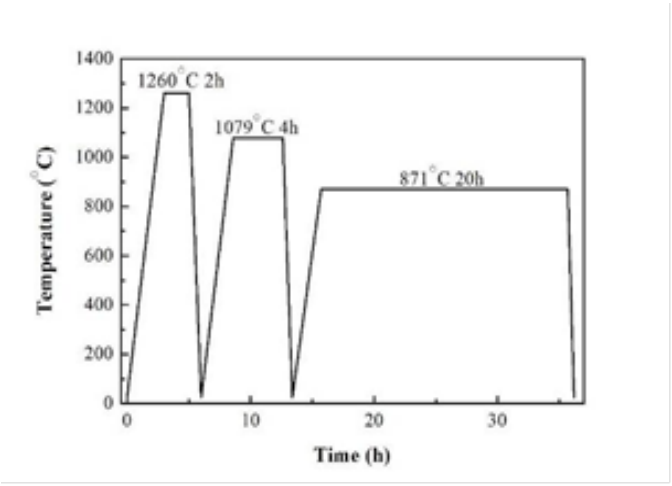
[10] H.E. Huand and C.H. Koo (2004), Characteristics and mechanical properties of polycrystalline CM247LC superalloy casting, *Mater. Trans.* vol. 45, no. 2, pp. 562-568.

表 1 CM247LC 與 MarM247 鎳基超合金成分表

	Ni	W	Co	Cr	Al	Ta	Hf	Ti	Mo	B	Zr	C
CM247LC	bal.	9.5	9.2	8.1	5.6	3.2	1.4	0.7	0.5	0.015	0.015	0.07
Mar-M247	bal.	10	10	8.3	5.5	3.0	1.5	1.0	0.7	0.015	0.050	0.15

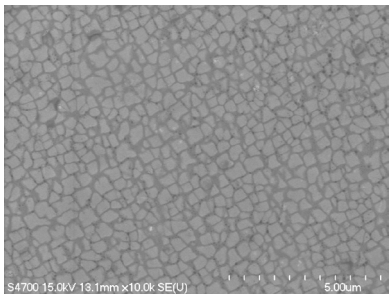
表 2 CM247LC 添加不同比例 Al 元素成分表

Alloy	Co	Al	Ti	Mo	W	Cr	Ta	Hf	B	Zr	C	Ni
CM247LC	9.2	5.67	0.7	0.5	9.5	8.1	3.2	1.44	0.016	0.007	0.07	Bal.
CM247LC with 0.5 wt.% Al addition	9.2	6.17	0.69	0.49	9.4	8.0	3.1	1.43	0.015	0.006	0.07	Bal.
CM247LC with 1 wt.% Al addition	9.2	6.67	0.69	0.49	9.3	8.0	3.1	1.42	0.015	0.006	0.07	Bal.
CM247LC with 1.5 wt.% Al addition	9.1	7.17	0.68	0.49	9.3	7.9	3.1	1.41	0.015	0.006	0.07	Bal.
CM247LC with 2 wt.% Al addition	9.1	7.67	0.68	0.48	9.2	7.9	3.1	1.40	0.015	0.006	0.07	Bal.

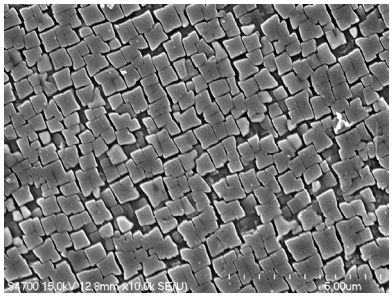


圖一 熱處理程序

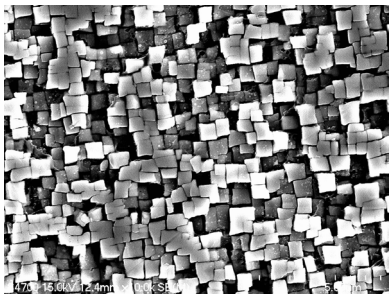
(1)



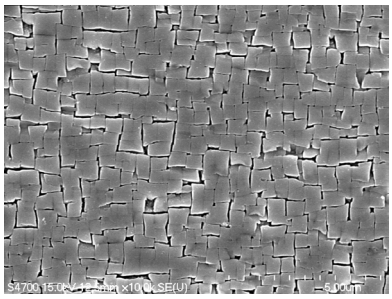
(2)



(3)



(4)



(5)

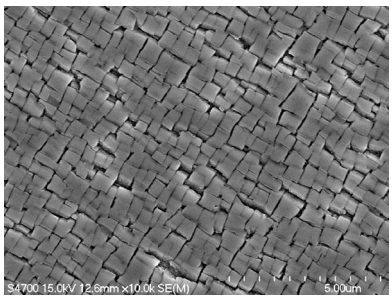
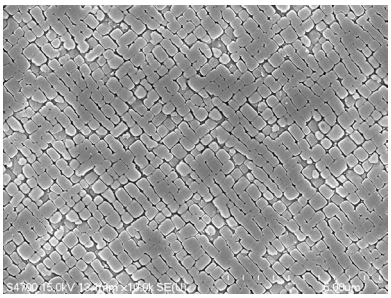
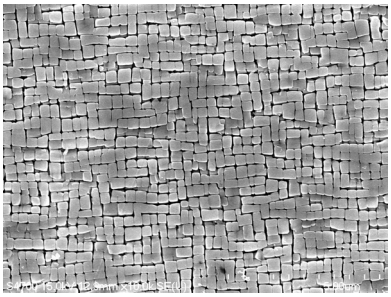


圖 2 未熱處理試片的微觀組織：
(1) 原料 CM247LC；(2)+0.5wt.%Al；
(3) +1wt.% Al；(4)+1.5wt.% Al；
(5) +2wt.% Al。

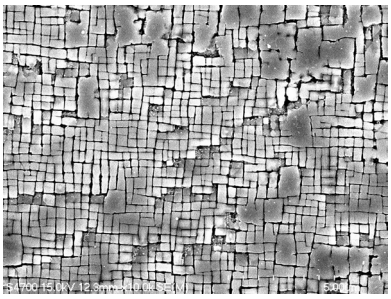
(1)



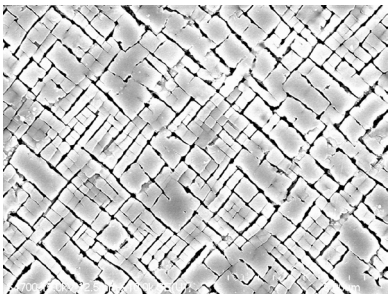
(2)



(3)



(4)



(5)

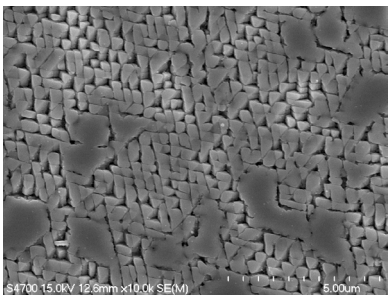
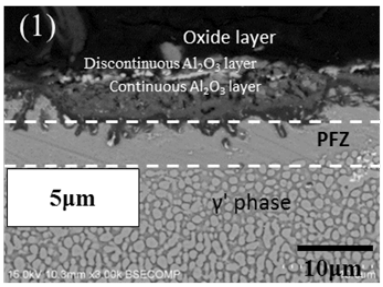
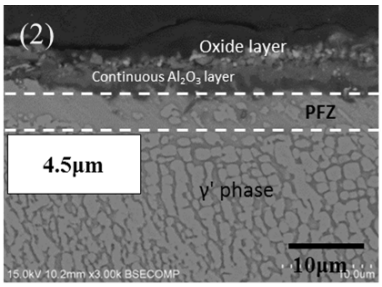


圖 3 經熱處理後試片的微觀組織：
(1) 原料 CM247LC；(2)+0.5wt.%Al；
(3) +1wt.% Al；(4)+1.5wt.% Al；
(5) +2wt.% Al。

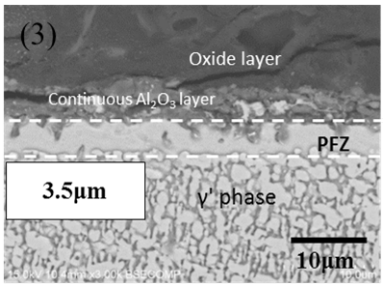
(1)



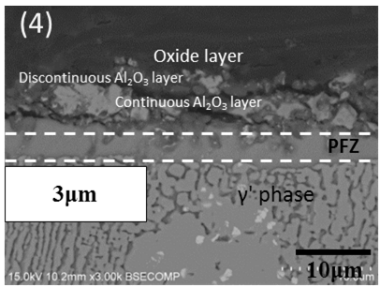
(2)



(3)



(4)



(5)

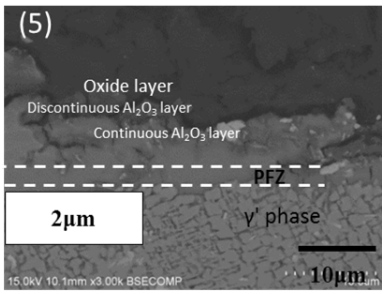
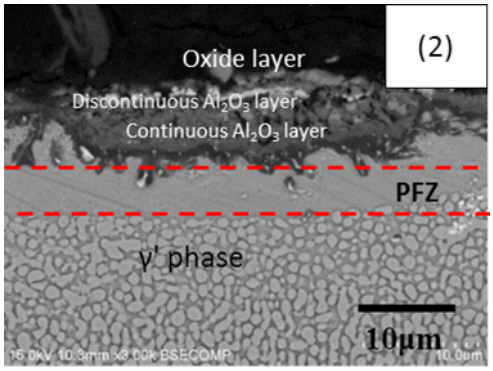
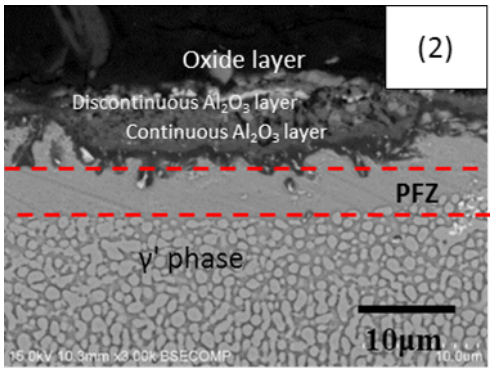


圖 4 高溫氧化 200 小時後試片剖面圖：(1) 原料 CM247LC；(2) +0.5wt.%Al；(3) +1wt.% Al；(4) +1.5wt.% Al；(5) +2wt.% Al。

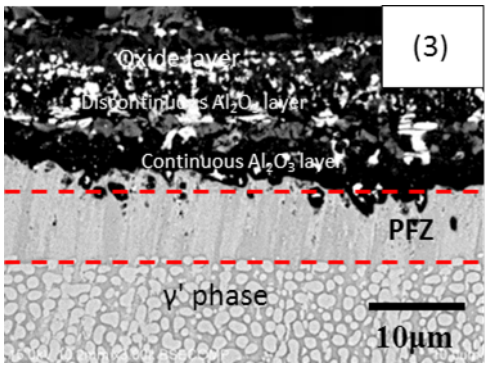
(1)



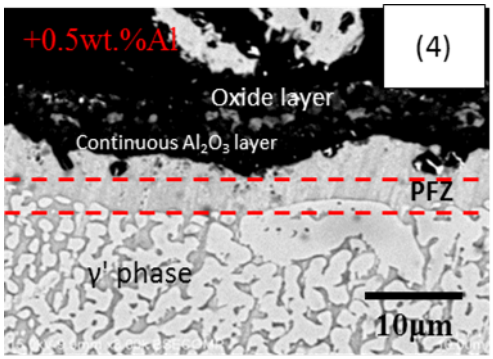
(2)



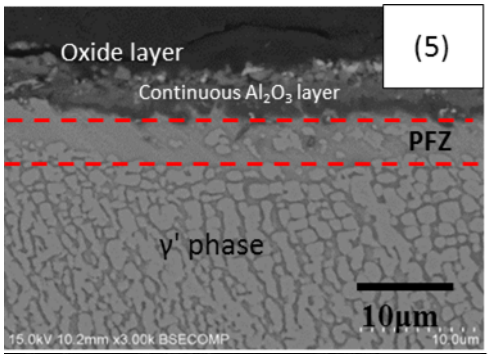
(3)



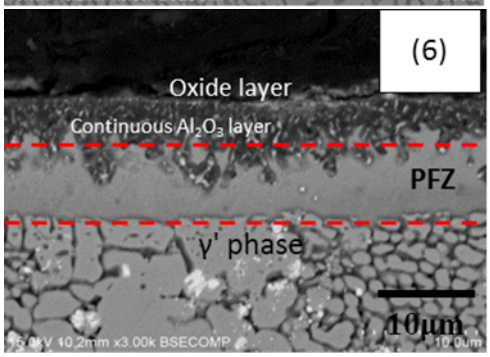
(4)



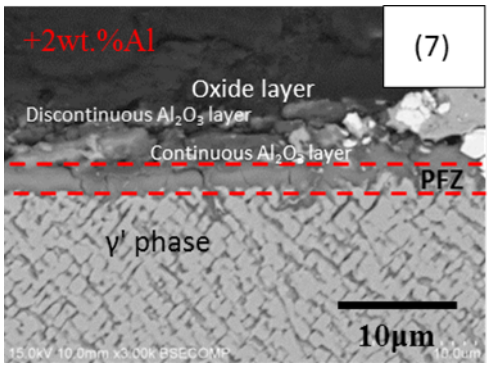
(5)



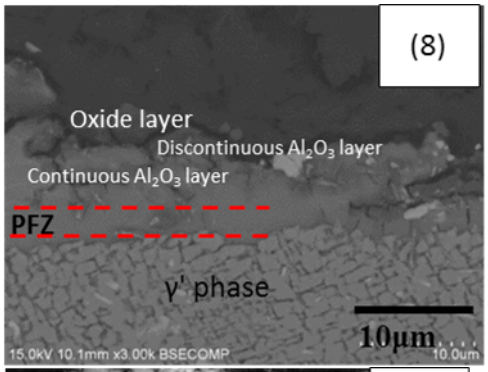
(6)



(7)



(8)



(9)

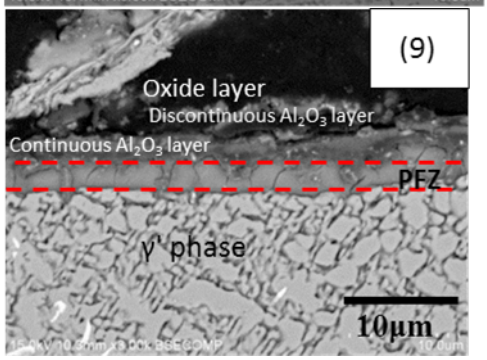


圖 5 高溫氧化原料 CM247LC、+0.5wt.%Al、+2wt.%Al 試片後剖面圖：
(1) (4) (7) 為 100 小時；(2) (5) (9) 為 200 小時；(3) (6) (9) 為 300 小時。

BACK

酒糟性皮膚炎影像診斷系統

黃柏翰[1] 張淑貞[2] 王智昱[3]

高雄長庚醫院美容中心、黃柏翰皮膚科診所[1]

大仁科技大學 餐旅管理系[2]

義守大學生物 醫學工程系[3]

摘要

本研究顯示一套以RBX分色影像為基礎的紅斑顏色鑑別系統，及其於酒糟性皮膚炎嚴重程度分級效果。以89位病患之極化光照片；照片先經RBX分色處理，去除黑色素影響後，再計算紅色影像之spectrum平均數，將之定義為「嚴重級分(degree of severity，DOS)」。結果顯示，酒糟愈嚴重之病患，其皮膚色愈顯暗沉，而DOS也趨向降低。此結果與醫師診斷結果相符。因此利用RBX分色影像以鑑別紅斑顏色，具有做為酒糟嚴重程度分類工具之潛力，可提供醫師客觀的指標以評估病情。

關鍵字：RBX影像系統、紅斑顏色鑑別、酒糟性皮膚炎、分級

前言

1.1 酒糟性皮膚炎之常用分類法則

酒糟性皮膚炎是一種常見的慢性皮膚病，好發部位通常在臉部，尤其是額頭、臉頰、下巴及鼻子的下半部位。其特徵為皮膚上持續或反覆地出現紅斑，伴隨微血管擴張，甚至發生丘疹或膿皰等。嚴重時不僅影響美觀，其所產生的不適或疼痛更造成病患痛苦。

酒糟性皮膚炎的嚴重程度，往往影響醫師採行的治療策略，因此如何將其正確分級，是治療酒糟性皮膚炎的一項重要課題。以Bamford等人為首的研究團隊進行的一項研究中，針對82位酒糟性皮膚炎病患，分析四位皮膚科醫師對這些病患所作的嚴重度分

級，與酒糟性皮膚炎的各項病徵(包含紅斑之顏色、丘疹/膿皰、以及皮膚組織增生情形)之相關性。結果發現，不論是全臉、前額、臉頰、鼻頭或是下巴，紅斑顏色之變化與嚴重程度分類的相關性都最高[1]。Tan等人則在2014年發表的文章中提及，五級分法(表一)對於酒糟性皮膚炎的分類而言，可靠度相當高[2]。然而每位醫師仍存在個體差異，且難以有統一的訓練過程。因此，發展一套標準的量測與分析工具，對於有心從事酒糟性皮膚炎嚴重程度分級的醫師及研究者，將會有很大的幫助[1]。

1.2 RBX分色影像應用於紅斑顏色鑑別

近年來有愈來愈多的研究顯示，有色人種中，包括非裔，拉美裔和亞裔等族群，發生酒糟性皮膚炎的情況也不在少數；但由於膚色往往容易掩蓋酒糟色澤的緣故，經常發生未確診或誤診的情況[3]。因此，為能正確運用前述CEA紅斑分級模式來進行酒糟性皮膚炎嚴重度評估，以進行正確之診斷，減少亞裔民族(包括台灣人)膚色之影響，將是十分重要的工作。

RBX分色影像係由美國Canfield Imaging Systems公司所開發的新技術，其原理為依據血紅蛋白與黑色素的散射光譜，將原始全彩影像分解為代表血紅蛋白散射光譜的Red(紅色)、代表黑色素散射光譜的Brown(棕色)，以及X(未定義)三個顏色向量空間[4]。圖一(a)顯示了RBX顏色向量空間(color space)的分解示意圖。此外，由於血紅蛋白與黑色素分布於皮膚的表面與深處，因此拍照時須使用極化光源，以取得不同深度的血紅蛋白與黑色素之散射光，並避免鏡面反射之干擾(圖一(b))。圖二則顯示了全彩影像以RBX顏色向量空間分解後之紅色(Red)以及棕色(Brown)影像。紅色可顯示臉部血紅蛋白之分布情形，棕色則顯示了黑色素的分布狀況。

國人膚色偏黃褐色，若是膚色較暗沉者，其臉部紅斑在照片中較不易清楚顯現，對於醫師分級診斷有一定程度的影響。本研究將探討利用RBX分色影像消除黑色素之影響後，紅色影像所呈現之訊息，是否與酒糟性皮膚炎嚴重程度相關，並進一步開發其分級演算法，以協助醫師快速精確地進行診斷。

實驗原理與方法

2.1 影像建立

為了解RBX分色影像對於皮膚酒糟嚴重程度分級的可行性，我們選取四張黃柏翰皮膚科診所病患所拍攝的相片來進行分析。照片以美國Canfield Scientific公司所生產之皮膚影像專用攝像機 (Reveal Imager, Canfield Scientific, Inc., Fairfield, NJ, USA) 來進行拍攝(圖四)。該攝像機可拍攝非極化光與極化光兩種照片。其中，非極化光照片可呈現目視時的皮膚影像狀況；而極化光照片則可消除反光的影響，並拍攝到較為深層的皮膚影像[5]。

拍攝時，先將患者頭部固定，並將臉部正對攝影機後，要求患者將眼睛閉上，避免強光傷害視網膜。拍攝時，以間隔約0.5秒的間隔拍攝非極化光與極化光照片各一張。照片拍攝完成之後，系統自動將極化光照片轉換為RBX分色影像，並產生紅色(Red)影像與棕色(Brown)影像。我們以紅色(Red)影像來進行酒糟嚴重程度分級之分析。

3.1.2 影像分析

我們以LabVIEW撰寫之程式來進行分析。圖四顯示分析程式介面。

結果與討論

3.1.3 酒糟性皮膚炎嚴重程度與皮膚顏色之關聯

由RBX之紅色(Red)影像可以看出，正常臉部皮膚影像呈現較淡的紅色；而酒糟程度愈嚴重，欲呈現暗紅的色澤。量化分析過程如下：我們在紅色(Red)影像之左頰選取一方型ROI區域，並計算該區域之三原色(紅、藍、綠)色板之spectrum(橫軸為亮度，縱軸則為像素數目)。從分析中發現，由於紅色為影像之主色，其差異性較不明顯；主要顏色區分則以藍色及綠色較為明顯；因此在此先期研究中，我們以藍色影像之spectrum作為主要之分析對象。接著我們計算藍色影像blue spectrum之平均值，以之作為酒糟嚴重程度分級之指標 (severity index)。圖五顯示，隨著酒糟嚴重程度增加，其severity index則顯著下降。該結果顯示，使用RBX分色影像來進行酒糟嚴重程度分級，並將之量化以提供病患參考，確為可行。

結論

本研究利用RBX分色影像以鑑別紅斑顏色之深淺，並用以分析酒糟性

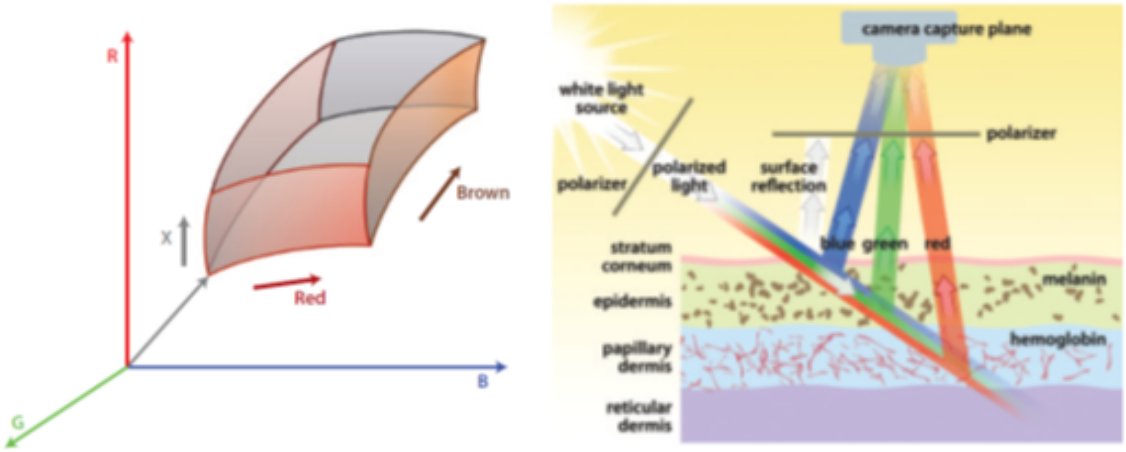
皮膚炎之嚴重程度。結果顯示，我們所設定之酒糟性皮膚炎嚴重程度，與資深專業醫師目視所得之嚴重程度有很好的關聯性。此結果可以幫助醫師制定酒糟性皮膚炎之嚴重程度的客觀鑑定標準，對於醫師之用藥與病患復原情形之判別具有極高的參考價值。

參考文獻

1. J.T. Bamford, C.E. Gessert,and C.M. Renier (2004), Measurement of the severity of rosacea, *J Am Acad Dermatol*, vol. 51, pp. 697-703.
2. J. Tan, H. Liu, J.J. Leyden,and M.J. Leoni (2014), Reliability of Clinician Erythema Assessment grading scale, *J Am Acad Dermatol*, vol. 71, pp. 760-763.
3. M. Communications (2008) Dr. Susan Taylor's BrownSkin.net http://www.brownskin.net/acne_rosacea.html.
4. R. Demirli, P. Otto, R. Viswanathan, and S. Patwardhan, Larkey J RBX™ Technology Overview. Canfield Imaging Systems.
5. A. Matsubara (2012) Differences in the surface and subsurface reflection characteristics of facial skin by age group, *Skin Research and Technology*, vol. 18, pp. 29-35.
6. Reveal imager(2014) http://www.canfieldsci.com/imaging-systems/reveal-imager/.

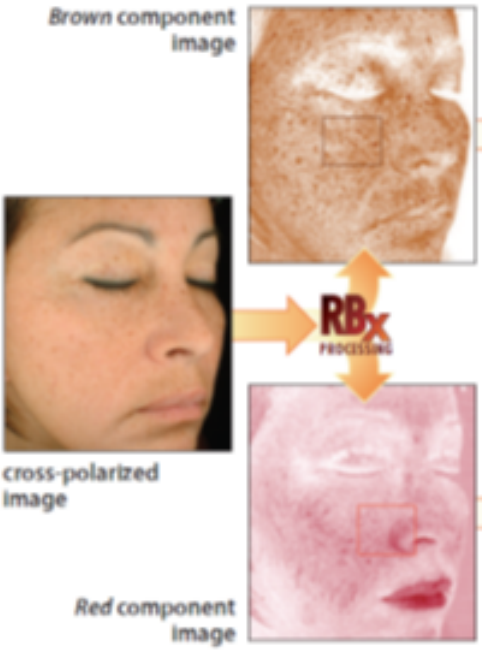
表一、CEA 五級分法 [2]

	CEA
0 = Clear	Clear skin with no signs of erythema
1 = Almost clear	Almost clear; slight redness
2 = Mild	Mild erythema, definite redness
3 = Moderate	Moderate erythema; marked redness
4 = Severe	Severe erythema; fiery redness



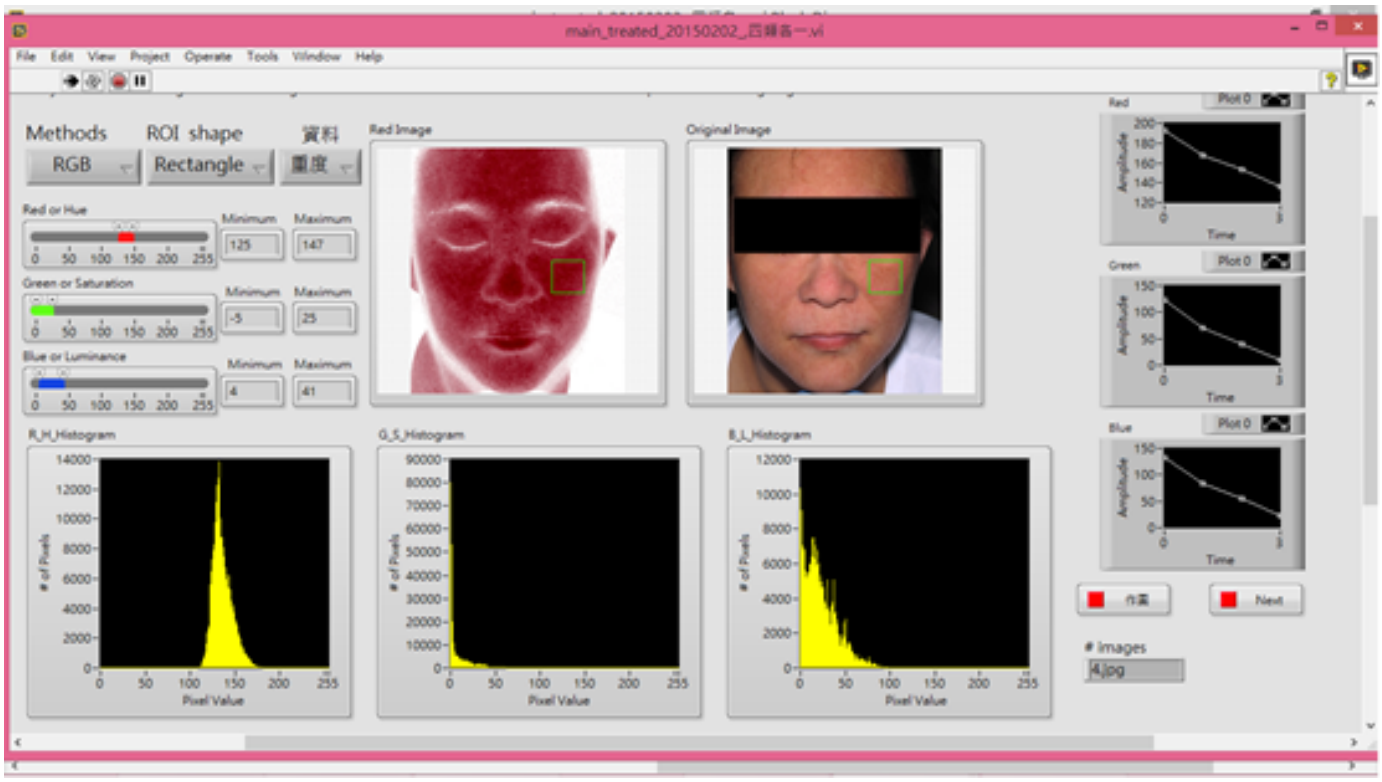
a b

圖一、(a) **RBX 顏色向量空間的分解示意圖；**(b) **極化光可取得較深皮膚影像** [4]

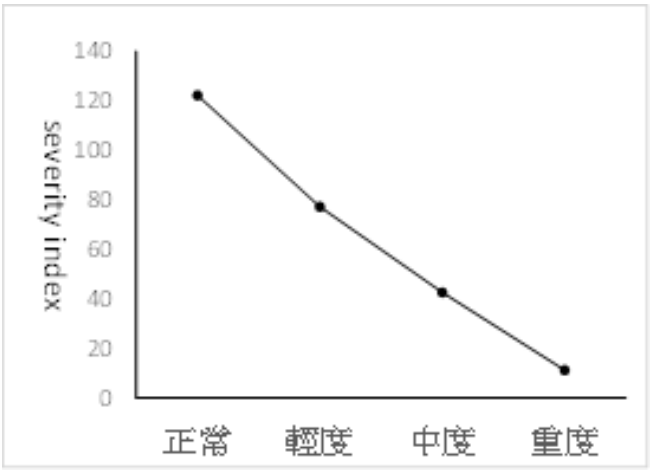


圖二、以極化光拍攝之全彩照片分解為紅色 (Red) 影像與棕色 (Brown) 影像 [4]

圖三、酒糟性皮膚炎造影系統 [6]



圖四、以 LabVIEW 撰寫之 RBX 分色影像酒糟嚴重程度分析程式介面



圖五、嚴重程度指標 (severity index) 與酒糟性皮膚炎嚴重程度呈現明顯的關聯性

BACK

平方剩餘碼解碼

僅以此文向Reed 教授致敬

李崇道[1]、張耀祖[2]

義守大學　通訊工程學系[1]

義守大學　財務與計算數學系[2]

摘要

實用而重要的Reed-Solomon碼的發明人Irving S. Reed 教授除了提出Reed-Solomon碼之外，還對一個碼平方剩餘碼有貢獻。平方剩餘碼雖然不是Reed 教授所提出，但在某種意義上說，他開啟了平方剩餘碼的解碼工作，在碼長103以內的12個二元平方剩餘碼中，除了碼長分別為7,17,23，最小的三個碼是比較簡單、已經有解碼法外，Reed 教授和他的學生們提出另外四個碼的解碼法，而剩下的五個碼長較大的碼的解碼法則是由義守大學的團隊完成。本篇是對二元平方剩餘碼的解碼工作做一個簡介。

注：在進入本文之前，先做一個說明，這裡所說的編碼，是錯誤更正碼（error correcting code，或譯為糾錯碼），不是大家比較熟悉的密碼(crypotgraphy)，兩者雖然都是對所要傳送的數位訊息做處理，然而目的不同，密碼編碼的目的是讓不受歡迎的接收者（就是侵入竊取訊息的人）無法得知訊息的內容；而糾錯編碼的目的則是保護所要傳送的資料，讓傳送資料過程中出現的錯誤能夠被接收者計算出並且剔除，而得到原始發送訊息。

前言

2011年9月，編碼發展史上的一位重要人物——美國的Reed教授 (Irving S. Reed, 1923.11.12-2011.9.11)與世長辭，標誌著代數編碼奠基的三位巨人（Claude Shannon, Richard Hamming, Reed）的一個階段的結束。

Reed 教授在1944年從加州理工學院數學系畢業，並在五年後，拿到數

學博士學位。在加州理工學院期間，他聽過近世代數的課程，後來也一直將學習近世代數作為業餘興趣，這可以說明，為什麼他是編碼發展史上考慮在有限體上做編碼[1]的先驅人物。

Reed教授對編碼的第一個貢獻是Reed-Muller碼(Reed-Muller codes)，Reed-Muller碼是美國的學者Muller在1954提出，同年Reed 教授提出不同的建構方式，並提出非常優異的解碼法，從此該碼被稱為Reed-Muller碼。在1969-1977年間，美國太空計畫的所有水手號(Mariner-class deep space probes)任務都是用Reed-Muller碼來保護所傳送的資料。

Reed教授對編碼的更大貢獻是，提出一個應用極為廣泛的Reed-Solomon碼(Reed-Solomon codes)。Reed-Solomon碼被用在深空通訊和各種商業應用中，從天王星、海王星傳回來的照片、影片，以及各種光碟 雷射唱片、DVD、藍光光碟等，可以說是應用中的糾錯碼極為重要的一種。

除了這兩個碼之外，還有一個碼平方剩餘碼(quadratic residue codes)，Reed 教授也做了重要意義的工作。在美國電子電機工程學會所出版的一本書《Reed-Solomon碼及其應用》（Reed-Solomon Codes and Their Applications, Eds. S.B. Wicker and V.K. Bhargava, IEEE Press, 1994），介紹Reed-Solomon碼的相關理論、軟硬體實現及其應用，書中第23頁提到：Reed 教授最近致力於平方剩餘碼解碼，（原文：“More recently Reed has focused his attention on the decoding of quadratic residue codes and the possible use of ideals in polynomial rings for this purpose.”）。

關於這一點，根據Reed 教授的學生 義守大學前電機資訊學院院長張肇健教授(T. K. Truong)說，Reed 教授覺得他提出了非二元碼中的最實用、最好的Reed-Solomon碼，他希望也能在二元碼部分有所貢獻。平方剩餘碼是二元碼中有著最好的距離性質的碼類（碼長103以內有12個二元平方剩餘碼，其中有9個具有最大的最小距離，較大的最小距離代表較高的糾錯能力，就是比較好的碼），而且平方剩餘碼的解碼極為困難，一直沒有好的解碼法；難解的好碼，引起了Reed 教授的興趣。

雖然平方剩餘碼不是Reed 教授所提出，但可以說是他開啟了平方剩餘碼的解碼工作，在碼長103以內的12個

二元平方剩餘碼中，除了碼長最小的三個是比較簡單、已經有解碼法外，Reed 教授和他的學生們提出4個碼的解碼法，而剩下的5個碼長較大的碼的解碼法則是由義守大學的團隊完成（外加一個碼長為113的碼）。本篇要對平方剩餘碼和它的解碼做一個簡介。

§二元平方剩餘碼簡介

二元平方剩餘碼是美國的Eugene Prange教授在1958年提出，是循環碼的一種，在二元線性碼當中，平方剩餘碼具有非常好的最小距離性質。其構造方法如下：

1.首先，平方剩餘碼的碼長n是一個被8除餘數為1或7的質數；符合這個條件的正整數由小到大依次為：

$$n = 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, 103, 113, \ldots$$

2.對於一個上述的碼長 n，找一個最小正整數 m，使得 n 能整除 $2^m - 1$；或說，m 為2在乘法群 $\boldsymbol{Z}_n^* = \{1,2,\ldots,n-1\}$ 中的秩(order)。

3.構造出含有2^m個元素的有限體 $E=GF(2^m)$。

4.若 $\alpha \in E$ 為E中非零元素所成乘法群的生成元，亦即 $E\backslash\{0\} = \langle\alpha\rangle$，

令 $\beta = \alpha^{\frac{2^m-1}{n}}$ 則 $\beta, \beta^2, \ldots, \beta^n \in E$ 為 x^n-1 的所有根。

5.考慮由所有模n的平方剩餘(quadratic residue modulo n)所成的集合：

$$Q_n = \{i^2 (\mathrm{mod}\, n) | i = 1, \ldots, n-1\}$$

6.考慮多項式 $g(x) = \prod_{i \in Q_n} (x - \beta^i)$

由上述步驟得到的多項式g(x)有下述兩個性質：

1. $g(x) \in F[x], F = GF(2)$
2. $g(x)$為 $x^n - 1$ 的因式

符合條件1和2的多項式可以做為循環碼(cyclic code)的生成多項式(generator polynomial)。

說明：第一個條件要求，碼長n被8除餘數為1或7，由數論的結果得知，有限體 $E = GF(2^m)$ 的特徵(characteristic) 2是模n的平方剩餘，亦即，$2 \in Q_n$，接著再推出，若 $i \in Q_n$，則 $2i \in Q_n$，由條件6可知，若 $\gamma = \beta^i$ 為生成多項式 $g(x)$的根，則 $\gamma^2 = (\beta^i)^2 = \beta^{2i}$ 也是 $g(x)$的根，因此$\gamma = \beta^i$ 的所有共軛根都是 $g(x)$的根，可得到，$\gamma = \beta^i$ 佈於 $F = GF(2)$ 的最小多項式 $min(\gamma, F)$ (minimal polynomial over F)是 $g(x)$ 的因式，因此 $g(x)$是它的某些根的最小多項式的乘積，所以，$g(x) \in F[x]$。另外，由條件6可知，$g(x)$的根也都是x^n-1的根，因此，$g(x)$為 x^n - 1 的因式。

範例1. 令 n=17，則 m=8 為2在乘法群 Z^*_{17} 中的秩，亦即，2^8-1為n=17的倍數。

若取 $f(x)=x^8+x^4+x^3+x^2+1$ 則 $f(x)\in F[x]$ 為本原多項式(primitive polynomial)，且

$$E=\{a_0+a_1\alpha+a_2\alpha^2+\cdots+a_7\alpha^7|a_0,\ldots,a_7\in F, f(\alpha)=0\}\cong\frac{F[x]}{\langle f(x)\rangle}$$

為擁有2^8=256個元素的有限體，其中元素α在乘法群中 $E^*=E\backslash\{0\}$ 的秩為2^8-1=255；令 $\beta=\alpha^{255/17}=\alpha^{15}$，則 $\beta^n=\beta^{17}=(\alpha^{15})^{17}=\alpha^{255}=1$ 亦即 $\beta\in E$ 為x^{17}-1的一個根，而且 $\beta,\beta^2,\ldots,\beta^{17}\in E$ 為x^{17}-1的所有根。

接著，模17的平方剩餘集為：

$$Q_{17}=\{i^2(\mathrm{mod}\ n)|i=1,\ldots,16\}=\{1,2,4,8,9,13,15,16\}$$

，因此，得到多項式

$$g(x)=\prod_{i\in Q_{17}}(x-\beta^i)=x^8+x^7+x^6+x^4+x^2+x+1$$

範例2. 若n=23，則m=11，取 $f(x)=x^{11}+x^4+x^3+x^2+1$，$\beta=\alpha^{(2^{11}-1)/23}=\alpha^{89}$，

$Q_{23}=\{i^2(\mathrm{mod}\ 23)|i=1,\ldots,22\}=$ {1,2,3,4,6,8,9,12,13,16,18} 得到

$g(x)=x^{11}+x^9+x^7+x^6+x^5+x+1$

用 $g(x)$當作生成多項式所得到的循環碼就叫做碼長為n的二元平方剩餘碼(binary quadratic residue code of length n)，通常簡稱為平方剩餘碼。其中，碼長為7和23的平方剩餘碼就是著名的漢明碼(Hamming code)和葛雷碼(Golay code)。

由於循環碼C的維數(dimension) k是碼長減去生成多項式的次數，

$k=n-\deg(g(x))$ 而 $g(x)$ 的次數等於平方剩餘集Q_n的元素個數（由於 $i^2(\mathrm{mod}\ n)=(-i)^2(\mathrm{mod}\ n)$，$Q_n$的元素個數為 $\frac{n-1}{2}$，因此，$k=n-\frac{n-1}{2}=\frac{n+1}{2}$，可得到平方剩餘碼的參數為$(n,k)=(n,\frac{n+1}{2})$，至於碼的最小距離$d$則沒有計算方式，只能按照最小距離的定義，一個碼一個碼去算。

附表1是部分已知的平方剩餘碼參數，表中在最小距離d打星號的就是有著最好的最小距離的平方剩餘碼，就是說在具有相同的(n,k)的分組碼(block codes)中，該平方剩餘碼的最小距離d最大。從表中可以看出，平方剩餘碼為什麼會被認為是好碼，原因是它們有著較大的最小距離，在碼不大於103的12個碼中有9個碼是最好的碼。

§二元平方剩餘碼的分類

平方剩餘碼按照生成多項式的可分解與否可分為兩型，在介紹兩型平方剩餘碼之前，先說明多項式的可分解性(irreducibility)。如同整數中的質數無法表示為兩個較小數的乘積一般，如果一個多項式 $f(x) \in F[x]$ 在 $F[x]$ 中無法表示為兩個次數較小多項式的乘積，就 $f(x)$ 稱為佈於 F 不可分解(irreducible over F)。

要留意的是，可分解與否是要看考慮哪種係數，也就是說在哪個體分解，例如 x^2+1 佈於實數 $F = \boldsymbol{R}$ 體 不可分解，佈於 $F = \boldsymbol{C}$ 複數體則是可分解。因此說不可分解要說明在哪個體。由於本篇文章都是考慮二元有限體 $GF(2)$，因此不再詳加說明，直接使用不可分解多項式這個詞。

定義：如果生成多項式 $g(x)$ 是一個不可分解多項式，則稱所生成的平方剩餘碼為第一型的平方剩餘碼(quadratic residue code of type I)，反之，若 $g(x)$ 為可分解多項式，則稱所生成的平方剩餘碼為第二型的平方剩餘碼(quadratic residue code of type II)。

平方剩餘碼是屬於哪一型？這個可以由碼長n來看出，其實是由模n平方剩餘集 Q_n 看出，如果模n平方剩餘集 Q_n 等於由2生成的循環子群 $\{2^1,2^2,\cdots\}$，則碼長為n的二元平方剩餘碼為第一型，否則為第二型。例如，

$$Q_7 = \{1,2,4\} = \{2^1 = 2, 2^2 = 4, 2^3 = 8 = 1\}$$

所以，碼長為7的二元平方剩餘碼為第一型。

用這個方法來看，第一型平方剩餘碼的碼長有：

7,17,23,41,47,71,79,97,103,…

第二型平方剩餘碼的碼長有：

31,73,89,113,…

兩種類型的平方剩餘碼在解碼的處理上會有不同，本文主要針對第一型二元平方剩餘碼。

接下來，介紹平方剩餘碼的編碼，由於平方剩餘碼是循環碼的一種，編碼方式和循環碼一樣，下面說明循環碼的編碼：

編碼(encode)：若循環碼C的參數為(n,k,d)，所謂**循環碼編碼**就是將訊息位元串中長度為k的二元位元串 $a_0,\cdots,a_{(k-1)}$ 當作多項式的係數，得到**訊息多項式**(information polynomial) a(x)：

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$$

然後將訊息多項式 $a(x)$ 乘上生成多項式 $g(x)$，所得到的多項式 $a(x)\,g(x)$ 稱為碼多項式(code polynonmial)，或稱

為碼字(codeword)，如下：

$$c(x) = a(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}$$

另外，碼多項式 $c(x)$的係數串 $c_0, \ldots, c_{n-1}$ 也叫做碼字。

接著，說明所謂訊息傳遞時發生的錯誤。實際通信的訊號傳遞是按時間來處理一個個位元，因此，如果發生錯誤，只是會將傳送的二元訊號0誤判為1，1誤判為0，不會發生傳送5個訊號，只收到3個訊號這種丟掉訊號的情形。

如果訊息傳送時是傳送碼字位元串 $c_0, \ldots, c_{n-1}$，而傳送過程出現一些錯誤，造成收到的位元串 $r_0, \ldots, r_{n-1}$ 和送出的碼字位元串 $c_0, \ldots, c_{n-1}$ 有些不同，如果對某個位置 $i \in \{0, 1, \ldots, n-1\}$，有 $r_i = c_i$，表示該位置沒有出錯，如果 $r_i \neq c_i$，則表示該位置出了錯；因此，令 $e_i = r_i - c_i, i \in \{0, 1, \ldots, n-1\}$ 稱所得到的位元串 $e_0, \ldots, e_{n-1}$ 為 **錯誤樣式** (error pattern)，並稱相應的多項式

$$e(x) = e_0 + e_1x + \cdots + e_{n-1}x^{n-1}$$

為錯誤多項式(error polynomial)，如果令 $r(x) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1}$，則有 $r(x) = c(x) + e(x)$。

範例3：考慮碼長n=17的平方剩餘碼

$n = 17(17,9,5)$

訊息位元串： $a(x) = x^4 + x^5 + x^8$

生成多項式：

$$g(x) = 1 + x + x^2 + x^4 + x^6 + x^7 + x^8$$

碼多項式：

$$c(x) = a(x)g(x) = x^4 + x^7 + x^{12} + x^{13} + x^{14} + x^{15} + x^{16}$$

錯誤多項式： $e(x) = x^3 + x^{14}$

接收多項式：

$$r(x) = c(x) + e(x) = x^3 + x^4 + x^7 + x^{12} + x^{13} + x^{15} + x^{16}$$

解碼(decode)：假設傳送出碼字 $c(x)$，而在傳遞的過程中發生了錯誤 $e(x)$，收到了 $r(x) = c(x) + e(x)$；所謂的**解碼**(decode)就是從所收到的 $r(x)$設法求出 $e(x)$，用來算出原來發送的碼字 $c(x) = r(x) - e(x)$。

解碼可以有不同的方法，可以用組合的方法，也可以用代數的方法，平方剩餘碼較有名的解碼方法有：1964年，日本的 Kasami 教授提出的error-trapping方法[2]，該方法適用於碼長較短的碼，如n=23,31，至於再大的碼，就要用代數的方法來解碼，就是下一節要介紹的代數解碼法。

§代數解碼法

(Algebraic decoding method)

所謂的代數解碼方法如下：先假設一個碼字 $c_0, \ldots, c_{n-1}$ 的傳送過程出現了v個位置的錯誤，也就是說錯誤多項

式 $e(x)$ 中有v個非零項，可以假設：

$e(x) = x^{l_1} + \cdots + x^{l_v}, 0 \le l_1 < \cdots < l_v < n$

而解碼就是求出錯誤所在的位置 $l_1, \ldots, l_v$

代數解碼法的作法是，將β代入錯誤多項式 $e(x)$，得到 $e(\beta) = \beta^{l_1} + \cdots + \beta^{l_v}$

然後，令 $Z_1 = \beta^{l_1}, \ldots, Z_v = \beta^{l_v}$ 所得到的 $Z_1, \ldots, Z_v$ 是有限體GF(2^m)中的元素，且 $Z_1, \ldots, Z_v$ 隱含了錯誤位置，稱它們為error-locator。

接著，考慮以 $Z_1^{-1} = \beta^{-l_1}, \ldots, Z_v^{-1} = \beta^{-l_v}$ 為根的多項式：$\sigma(x) = (1 - Z_1 x) \cdots (1 - Z_v x)$

稱 $\sigma(x)$ 為 $e(x)$ 的錯誤位置多項式(error-locator polynomial)。為什麼不直接用 $Z_1, \ldots, Z_v$ 當作根，而用他們的反元素的原因是，考慮非二元的情形，不但要決定錯誤的位置，還要決定錯誤的值，這麼定義，便於發展求錯誤值的作法。

根據定義，如果能求出錯誤位置多項式 $\sigma(x)$ 就很容易得到錯誤位置 $l_1, \ldots, l_v$。說容易的原因是，雖然一般多項式求根公式只到4次，但是錯誤位置多項式 $\sigma(x)$ 不是一般多項式，$\sigma(x)$ 的根只能為集合 $\{\beta^0, \beta^{-1}, \ldots, \beta^{-(n-1)}\}$ 中的元素，因此逐一代入集合中的元素，便可找到 $\sigma(x)$ 的所有根，而知道錯誤位置：由於 $\beta^n = 1$，因此 $\beta^{-i} = \beta^{n-i}$，如果 $\sigma(\beta^{n-i}) = 0$，則表示有一個error locator錯誤位置為 $Z_* = \beta^i$，或是說x^i是錯誤多項式 $e(x)$ 中的一項。這個雖然簡單卻是極為有用的作法是華裔學者錢聞天提出來的，也被稱為**錢氏搜尋法**(Chien Search)。有這個錢氏搜尋法，代數解碼法的最主要工作就是求出錯誤位置多項式 $\sigma(x)$。

若錯誤多項式 $e(x)$ 有 v 個錯誤，則錯誤位置多項式 $\sigma(x)$ 有 v 個根，因此是一個v次多項式，可將錯誤位置多項式 $\sigma(x)$ 表示如下：

$\sigma(x) = \sigma_0 + \sigma_1 x + \cdots + \sigma_{v-1} x^{v-1} + \sigma_v x^v$

由 $\sigma(x)$ 的定義 $\sigma(x) = (1 - Z_1 x) \cdots (1 - Z_v x)$，可得到下列根與係數的關係：

x^0的係數： $\sigma_0 = 1$

x^1的係數： $\sigma_1 = (-1)(Z_1 + \cdots + Z_v) = (-1)\sum_{i=1}^{v} Z_i$

x^2的係數： $\sigma_2 = (-1)^2(Z_1 Z_2 + \cdots + Z_{v-1} Z_v) = (-1)^2 \sum_{i<j} Z_i Z_j$

$\vdots$

x^k的係數： $\sigma_k = (-1)^k \sum_{i_1 < i_2 < \cdots < i_k} Z_{i_1} \cdots Z_{i_k}$

$\vdots$

x^v的係數： $\sigma_v = (-1)^v Z_1 \cdots Z_v$

從中可以看出每一個係數 $\sigma_i, i = 1, \ldots, v-1$ 都是以 $Z_1, \ldots, Z_v$ 為變數的對稱函數，這些稱為**基本對稱函數**(elementary symmetric functions)。

另外，分別將 $\beta^i, i = 1, \ldots, n-1$ 代入錯誤多項式 $e(x)$，可得到

$e(\beta^i) = (\beta^i)^{l_1} + \cdots + (\beta^i)^{l_v} = (\beta^{l_1})^i + \cdots + (\beta^{l_v})^i = (Z_1)^i + \cdots + (Z_v)^i$ 稱之為錯誤多項式 $e(x)$ 的第i個症狀子(i-th syndrome)，記為S_i，下面為所有的症狀子：

$$S_1 = e(\beta) = Z_1 + \cdots + Z_v$$
$$S_2 = e(\beta^2) = (Z_1)^2 + \cdots + (Z_v)^2$$
$$\vdots$$
$$S_{n-1} = e(\beta^{n-1}) = (Z_1)^{n-1} + \cdots + (Z_v)^{n-1}$$

這些全都是以 $Z_1, \ldots, Z_v$ 為變數的對稱函數，稱它們為**冪和對稱函數**(power-sum symmetric functions)。

冪和對稱函數和基本對稱函數之間有一種關係，稱之為牛頓等式(Newton identities)，其在二元有限體的簡化形式如下：

$$S_1 + \sigma_1 = 0$$
$$S_3 + \sigma_1 S_2 + 2\sigma_2 = 0$$
$$S_3 + \sigma_1 S_2 + \sigma_2 S_1 + \sigma_3 = 0$$
$$S_5 + \sigma_1 S_4 + \sigma_2 S_3 + \sigma_3 S_2 + \sigma_4 S_1 + \sigma_5 = 0$$
$$\vdots$$
$$S_i + \sum_{j=1}^{i-1} \sigma_j S_{i-j} + \sigma_i = 0 \quad (1 \le i \le v, i = \text{奇數})$$
$$S_i + \sum_{j=1}^{v} \sigma_j S_{i-j} = 0 \quad (i > v, i = \text{奇數})$$

如果知道所有的症狀子的值，利用牛頓等式及各症狀子的值，便可以求得錯誤位置多項式的係 $\sigma_1, \ldots, \sigma_v$ 數 ，因而可得到錯誤多項式 $\sigma(x)$ 。

問題是，不會是所有症狀子的值都可以求出。對於平方剩餘碼來說，當 $i \in Q_n$ 時，症狀子S_i的值可由收到的 $r(x)$ 代入 β^i 而得到：

$$r(\beta^i) = c(\beta^i) + e(\beta^i) = 0 + e(\beta^i) = e(\beta^i) = S_i, i \in Q_n$$

因此若 $i \in Q_n$ ，稱S_i 為**已知症狀子**(known syndrome)；而 i不屬於Q_n 時，症狀子S_i的值無法由收到的$r(x)$來得出，稱之為**未知症狀子**(unknown syndrome)。

由症狀子的定義可以看出，各個症狀子的值之間有一個關係，有於是在二元有限體，對任意 $i \in \{1, \ldots, n-1\}$

$$S_{2i} = e(\beta^{2i}) = Z_1^{2i} + \cdots + Z_v^{2i} = (Z_1^i + \cdots + Z_v^i)^2 = S_i^2$$

在第一型平方剩餘碼的情形，由於 $Q_n = \{1, 2^1, 2^2, \ldots, 2^{\frac{n-3}{2}}\}$ ，因此所有的已知症狀子都是S_1的冪次方，值都可由S_1決定，因此稱S_1為**主要已知症狀子**(primary known syndrome)。如果r是非平方剩餘集合中最小的，則非平方剩餘集可以表為：

$$rQ_n = \{r \times 1, r \times 2^1, r \times 2^2, \ldots, r \times 2^{\frac{n-3}{2}}\}$$

因此，所有未知症狀子也是可以表為S_r的冪次方，所以S_r稱為**主要未知症狀子**(primary unknown syndrome)。

例如，n=7，平方剩餘集 $Q_7 = \{1,2,4\}$ ，

而 $3Q_7=\{3,6,12\}=\{3,6,5\}$ 非平方剩餘集。同時，有已知症狀子的關係：$S_2=S_1^2, S_4=S_1^4$，以及未知症狀子的關係 $S_6=S_3^2, S_5=S_3^4$。

當已知症狀子夠多，還是可以用牛頓等式來解碼；早期解平方剩餘碼，由於碼長較小，錯誤數量不多，就是用這種方法求得錯誤位置多項式 $\sigma(x)$。下面用碼長23的平方剩餘碼，也就是所謂的Golay碼[3]來做說明。

範例4：考慮碼長n=23的平方剩餘碼，因 $Q_{23}=\{1,2,3,4,6,8,9,12,13,16,18\}$，表示 S_1, S_3, S_9 是已知症狀子。下表列出不同數量錯誤時的牛頓等式及求得的錯誤位置多項式：

例如，v=2 時，假設 $e(x)=x^3+x^{11}$，則

$$S_1=e(\beta)=e(\alpha^{89})=(\alpha^{89})^3+(\alpha^{89})^{11}=\alpha^{342}$$

$$S_3=S_1^{256}=\alpha^{1578}$$

由表中公式計算的σ_2的值：

$$\sigma_2=(S_3+S_1{}^3)/S_1=(\alpha^{1578}+(\alpha^{342})^3)/\alpha^{342}$$
$$=\alpha^{1588}/\alpha^{342}=\alpha^{1246}$$

而根據 $\sigma(x)$ 的定義計算係數σ_2：

$$\sigma_2=\beta^3\cdot\beta^{11}=(\alpha^{89})^{14}=\alpha^{1246}$$

例如，v=3 時，假設 $e(x)=1+x^{10}+x^{19}$，則 $S_1=e(\beta)=e(\alpha^{89})=$

$$1+(\alpha^{89})^{10}+(\alpha^{89})^{19}=\alpha^{1593}$$

$S_3=S_1^{256}=\alpha^{455}$，$S_9=S_1^{32}=\alpha^{1848}$,

因此

$$D=(\alpha^{455}+(\alpha^{1593})^3)^2+(\alpha^{1848}+(\alpha^{1593})^9)/(\alpha^{455}+(\alpha^{1593})^3)$$
$$=\alpha^{1829}+\alpha^{1637}/\alpha^{1938}=\alpha^{635}$$

$$D^{1/3}=\alpha^{(1976+2047)/3}=\alpha^{894}$$

由表中公式計算出來的值：

$$\sigma_1=(S_3+S_1D^{1/3})=\alpha^{1848}+\alpha^{1593}\alpha^{894}=\alpha^{534}$$

$$\sigma_2=(S_1{}^2+D^{1/3})=(\alpha^{1593})^2+\alpha^{894}=\alpha^{1593}$$

而根據 $\sigma(x)$ 的定義計算係數

$$\sigma_1=1+\beta^{10}+\beta^{19}=1+(\alpha^{89})^{10}+(\alpha^{89})^{19}=\alpha^{1593}$$

$$\sigma_2=1\cdot\beta^{10}+1\cdot\beta^{19}+\beta^{10}\cdot\beta^{19}=$$
$$(\alpha^{89})^{10}+(\alpha^{89})^{19}+(\alpha^{89})^{29}=\alpha^{515}$$

早期解平方剩餘碼，對於碼長為23,31,41,73的情形[4-6]，都是透過解牛頓等式的方法而解出的。然而，這個方法會隨著碼長增加，而已知症狀子變得相對不足，因而無法解碼，下一節介紹一種方法可以部份解決這個問題。

§未知症狀子表示法

(Unknown syndrome representation method)

在[7]的論文中，對於碼長為47的平方剩餘碼，在五個錯 v=5 的時候，出現已知症狀子不夠的情形，論文中用了一個額外的技巧，將未知症狀子

表為已知症狀子的函數來增加已知症狀子的數量，最後完成解碼。其作法如下：

1.要求未知症狀子S_r的表示式，先考慮集合 $Q_n^r = Q_n \cup \{0,r\}$

2.假設錯誤多項式的錯誤數量為v，從集合Q_n^r中找到兩個各有v+1個元素的集合I和J

$$I = \{i_1, \ldots, i_{v+1}\},\ J = \{j_1, \ldots, j_{v+1}\}$$

3.根據這兩個集合，做出兩個矩陣$X(I)$和$X(J)$

$$X(I) = \begin{bmatrix} Z_1^{i_1} & \cdots & Z_v^{i_1} \\ \vdots & \ddots & \vdots \\ Z_1^{i_{v+1}} & \cdots & Z_v^{i_{v+1}} \end{bmatrix}, X(J) = \begin{bmatrix} Z_1^{j_1} & \cdots & Z_v^{j_1} \\ \vdots & \ddots & \vdots \\ Z_1^{j_{v+1}} & \cdots & Z_v^{j_{v+1}} \end{bmatrix}$$

可以看出，兩個矩陣的大小都是$(v+1)\times v$，

4.接著考慮下面的矩陣

$$S(I,J) = X(I)X(J)^t$$

其中，$X(J)^t$表示 $X(J)$的轉置矩陣(transpose)；得到的$S(I,J)$是一個$(v+1)\times(v+1)$的方陣，其$(1,1)$位置的陣元(entry)是$X(I)$的第一列(row)和$X(J)$的第一列的向量內積，如下：

$$\left(Z_1^{i_1}, \ldots, Z_v^{i_1}\right)\left(Z_1^{j_1}, \ldots, Z_v^{j_1}\right) = Z_1^{i_1+j_1} + \cdots + Z_v^{i_1+j_1} = S_{i_1+j_1}$$

因此，方陣$S(I,J)$可表示如下：

$$S(I,J) = \begin{bmatrix} S_{i_1+j_1} & \cdots & S_{i_1+j_{v+1}} \\ \vdots & \ddots & \vdots \\ S_{i_{v+1}+j_1} & \cdots & S_{i_{v+1}+j_{v+1}} \end{bmatrix}$$

由於矩陣$X(I)$和$X(J)$都是$(v+1)\times v$的矩陣，它們的秩(rank)都不會超過v，因此方陣$S(I,J)$的秩也不會超過v，所以$S(I,J)$的行列式為0，

$$\det\left(S(I,J)\right) = 0$$

如果$S(I,J)$的陣元中只有一個未知症狀子S_r，其他的陣元都是已知症狀子，則由$\det\left(S(I,J)\right) = 0$，未知症狀子$S_r$可以表為那些已知症狀子的函數，解碼時未知症狀子$S_r$的值就可以由那些已知症狀子的值代入所得到的函數而求得。詳細作法可參考下面的範例。

範例5. 考慮碼長為17的平方剩餘碼，由範例1可知Q_{17}={1,2,4,8,9,13,15,16}，未知症狀子為S_3，因此有

$$Q_n^3 = \{0,1,2,3,4,8,9,13,15,16\}$$

假設有兩個錯，v=2；若取

$I = \{0,1,3\}, J = \{0,1,15\}$則有

$$X(I) = \begin{bmatrix} Z_1^0 & Z_2^0 \\ Z_1^1 & Z_2^1 \\ Z_1^3 & Z_2^3 \end{bmatrix}, X(J) = \begin{bmatrix} Z_1^0 & Z_2^0 \\ Z_1^1 & Z_2^1 \\ Z_1^{15} & Z_2^{15} \end{bmatrix},$$

$$S(I,J) = X(I)X(J)^t = \begin{bmatrix} S_0 & S_1 & S_3 \\ S_1 & S_2 & S_4 \\ S_{15} & S_{16} & S_1 \end{bmatrix}$$

可以看出，矩陣$S(I,J)$的陣元中只有(1,3)位置的陣元是未知症狀子S_3，其餘的都是已知症狀子。而$S(I,J)$的行列式為

$$\det\left(S(I,J)\right) = (S_0S_2S_1 + S_1S_4S_{15} + S_1S_{16}S_3) - (S_3S_2S_{15} + S_1S_1S_1 + S_0S_{16}S_4)$$

由於 $\det(S(I,J))=0$ 由上式整理可得

$$S_3=\frac{S_0S_2S_1+S_1S_4S_{15}-S_1S_1S_1-S_0S_{16}S_4}{S_2S_{15}-S_1S_{16}}$$

由於v=2，S_0的值計算如下：

$$S_0=e(\beta^0)=e(1)=(1)^3+(1)^{14}=0$$

再加上一些已知結果：

$$S_2=S_1^2,S_4=S_1^4,S_{16}=S_1^{16},S_{15}=S_1^{32}$$

因此，可進一步簡化S_3的公式：

$$S_3=\frac{S_1S_4S_{15}+S_1S_1S_1}{S_2S_{15}+S_1S_{16}}$$

$$=\frac{S_1S_1^4S_1^{32}+S_1^3}{S_1^2S_1^{32}+S_1S_1^{16}}=\frac{S_1^{37}+S_1^3}{S_1^{34}+S_1^{17}}$$

這就是說，假設錯誤多項式有兩個錯的時候，未知症狀子S_3的值可以用已知症狀子S_1經由上述公式求出。

例如，假設$e(x)=x^3+x^{14}$，則

$$S_1=e(\beta)=e(\alpha^{15})=(\alpha^{15})^3+(\alpha^{15})^{14}=\alpha^{17}$$

由公式計算S_3的值：

$$\frac{(\alpha^{17})^{37}+(\alpha^{17})^3}{(\alpha^{17})^{34}+(\alpha^{17})^{17}}=\frac{\alpha^{629}+\alpha^{51}}{\alpha^{578}+\alpha^{289}}=\frac{\alpha^{68}}{\alpha^{170}}=\alpha^{153}$$

而根據定義計算S_3的值：

$$S_3=e(\beta^3)=e(\alpha^{45})=(\alpha^{45})^3+(\alpha^{45})^{14}=\alpha^{153}$$

用這種方法，再加上一點技巧，是解決了碼長47平方剩餘碼的解碼。然而，當碼長變大，錯誤數量變多時，要找到合適的集合I和J，使得矩陣$S(I,J)$中只有一個未知症狀子S_r，就會更加困難，即使找到，也求得未知症狀子表示法，要求解牛頓等式將也是極為困難。為此，我們發展了下一節的解碼法。

§Berlekamp-Massey算法

要求得錯誤位置多項式σ(x)，還有一種作法，由著名編碼學者Berlekamp在他的名著Algebraic coding theory一書中提出，沒有發表論文；後來另外一位著名編碼學者Massey 從線性移位暫存器(linear shift-register)的角度詮釋Berlekamp的方法，讓該方法更容易理解，現在這個方法被稱為Berlekamp-Massey算法。

Berlekamp-Massey算法是一個非常有效率的解碼算法，原本是用來解BCH碼(Bose-Chaudhuri-Hocquenghem codes)。BCH碼也是循環碼的一種，可以說是循環碼、甚至是線性分組碼中應用最為廣泛的一種，從太空中的衛星通訊到地面上的行動通訊都可應用BCH碼；BCH碼之所以會被廣泛應用的原因，就是因為有Berlekamp-Massey算法這個良好的解碼算法。

然而使用Berlekamp-Massey算法的條件是：要解t個錯，必須有$2t$個連續的已知症狀子，而BCH碼就能提供$2t$個已知症狀子。

相較之下，平方剩餘碼無法提供2t

個連續的已知症狀子，例如，n=23，$Q_{23}=\{1,2,3,4,6,8,9,12,13,16,18\}$，因此，最多的連續已知症狀子為 S_1,S_2,S_3,S_4，只有四個，而碼長為23的平方剩餘碼能解3個錯，若要用Berlekamp-Massey算法解3個錯，必須要有6個連續的已知症狀子，缺了一個未知症狀子S_5的值。如果用上述的方法，將未知症狀子S_5表為已知症狀子S_1的函數，就會有6個連續的已知症狀子的值，就可以用Berlekamp-Massey算法來解碼。

根據上面的想法，我們可以發展出一個第一型平方剩餘碼的解碼算法，如下：

1.收到 $r(\beta)$，計算主要已知症狀子 $S_1=r(\beta)$：
如果 $S_1=0$，表示 $e(x)=0$，不需要解碼，直接進入步驟12
如果 $S_1\neq 0$，表示 $e(x)\neq 0$，進入下一步驟。
2.令v=1
3.假設錯誤多項式中有v個錯，並使用未知症狀子表示法 $S_r=S_r^{(v)}$
4.用兩個主要症狀子 $S_1,S_r^{(v)}$ 計算出2t個連續的症狀子：$S_1,\ldots,S_{2t}$
5.使用Berlekamp-Massey算法，得出錯誤位置多項式：$\sigma^{(v)}(x)$
6.如果 $\sigma^{(v)}(x)$ 的次數等於v，則進入第8步驟；
7.令v=v+1：
如果v≤t，回到第3步驟；
如果v>t，代表 $e(x)$ 不可解，前進到第12步驟
8.使用錢氏搜尋法求得v'個錯誤位置：$l_1,\ldots,l_{v'}$
9.如果v'<v，回到第7步驟
10.得到錯誤多項式：$e(x)=x^{l_1}+\cdots+x^{l_v}$
11.得到原發送的碼字為：$c(x)=r(x)-e(x)$
12.解碼完成

用一個例子來說明上述解碼算法：

範例6：考慮碼長為17的平方剩餘碼，假設碼多項式為

$$c(x)=x^4+x^7+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}$$

而錯誤多項式為 $e(x)=x^3+x^{10}$，則接收多項式

$$r(x)=c(x)+e(x)=$$
$$x^3+x^4+x^7+x^{10}+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}$$

使用上述解碼算法的解碼過程如下：

步驟1：計算第一症狀子

$$S_1=r(\beta)=\beta^3+\beta^4+\beta^7+\beta^{10}+\beta^{12}+\beta^{13}$$
$$+\beta^{14}+\beta^{15}+\beta^{16}=\alpha^{38}\neq 0$$

進入第2步驟

步驟2：令v=1

步驟3：計算未知症狀子

$$S_3=S_1^3=(\alpha^{38})^3=\alpha^{114}$$

步驟4：計算出2t=4個連續的症狀子：

S_1, S_2, S_3, S_4

$S_1 = \alpha^{38},\ S_2 = S_1^2 = (\alpha^{38})^2 = \alpha^{76},$

$S_3 = \alpha^{114},\ S_4 = S_2^2 = (\alpha^{76})^2 = \alpha^{152}$

步驟5：用Berlekamp-Massey演算法求得：$\sigma(x) = 1 - \alpha^{38}x$

步驟6：$\sigma^{(v)}(x)$的次數等於v=1，進入第8步驟

步驟8：用錢氏搜尋法逐一將 $\beta^0, \ldots, \beta^{-16}$ 代入$\sigma(x)$找其根：

$\sigma(\beta^0) = 1 - \alpha^{38}\beta^0 \neq 0$

$\sigma(\beta^{-1}) = 1 - \alpha^{38}\beta^{-1} \neq 0$

$\sigma(\beta^{-2}) = 1 - \alpha^{38}\beta^{-2} \neq 0$

$\sigma(\beta^{-4}) = 1 - \alpha^{38}\beta^{-4} \neq 0$

$\sigma(\beta^{-5}) = 1 - \alpha^{38}\beta^{-5} \neq 0$

$\sigma(\beta^{-6}) = 1 - \alpha^{38}\beta^{-6} \neq 0$

$\sigma(\beta^{-7}) = 1 - \alpha^{38}\beta^{-7} \neq 0$

$\sigma(\beta^{-8}) = 1 - \alpha^{38}\beta^{-8} \neq 0$

$\sigma(\beta^{-9}) = 1 - \alpha^{38}\beta^{-9} \neq 0$

$\sigma(\beta^{-10}) = 1 - \alpha^{38}\beta^{-10} \neq 0$

$\sigma(\beta^{-11}) = 1 - \alpha^{38}\beta^{-11} \neq 0$

$\sigma(\beta^{-12}) = 1 - \alpha^{38}\beta^{-12} \neq 0$

$\sigma(\beta^{-13}) = 1 - \alpha^{38}\beta^{-13} \neq 0$

$\sigma(\beta^{-14}) = 1 - \alpha^{38}\beta^{-14} \neq 0$

$\sigma(\beta^{-15}) = 1 - \alpha^{38}\beta^{-15} \neq 0$

$\sigma(\beta^{-16}) = 1 - \alpha^{38}\beta^{-16} \neq 0$

根據以上結果可知 $v' = 0$

步驟9：$0 = v' < v = 1$，回到第7步驟

步驟7：令v=2

步驟8：v=t=2，回到第3步驟

步驟3：計算未知症狀子(根據範例3)

$S_3 = ((\alpha^{38})^{37} + (\alpha^{38})^3)/((\alpha^{38})^{34} + (\alpha^{38})^{17}) = \alpha^{182}/\alpha^{170} = \alpha^{12}$

步驟4：計算出2t=4個連續的症狀子：S_1, S_2, S_3, S_4

$S_1 = \alpha^{38}, S_2 = S_1^2 = (\alpha^{38})^2 = \alpha^{12},$

$S_3 = \alpha^{114}, S_4 = S_2^2 = (\alpha^{76})^2 = \alpha^{152}$，

步驟5：用Berlekamp-Massey演算法求得：$\sigma(x) = 1 - \alpha^{38}x + \alpha^{195}x^2$

步驟6：$\sigma^{(v)}(x)$的次數等於v=2，進入第8步驟

步驟8：用錢氏搜尋法逐一將 $\beta^0, \ldots, \beta^{-16}$ 代入$\sigma(x)$找其根

$\sigma(\beta^0) = 1 - \alpha^{38}(\beta^0) + \alpha^{195}(\beta^0)^2 = \alpha^{174} \neq 0$

$\sigma(\beta^{-1}) = \alpha^{210}, \sigma(\beta^{-2}) = \alpha^{42},$

$\sigma(\beta^{-3}) = 0 \Rightarrow l_1 = 3$

$\sigma(\beta^{-4}) = \alpha^{80},\ \sigma(\beta^{-5}) = \alpha^{235}, \sigma(\beta^{-6}) = \alpha^{11},$

$\sigma(\beta^{-7}) = \alpha^{103}, \sigma(\beta^{-8}) = \alpha^{190}, \sigma(\beta^{-9}) = \alpha^{5},$

$\sigma(\beta^{-10}) = 0 \Rightarrow l_2 = 10$

$\sigma(\beta^{-11}) = \alpha^{162}, \sigma(\beta^{-12}) = \alpha^{45}, \sigma(\beta^{-13}) = \alpha^{234},$

$\sigma(\beta^{-14}) = \alpha^{134}, \sigma(\beta^{-15}) = \alpha^{68}, \sigma(\beta^{-16}) = \alpha^{104}.$，

根據以上結果可知v'=2，錯誤位置l_1=3, l_2=10。

步驟9：v'<v不成立

步驟10：得到錯誤多項式：$e(x) = x^3 + x^{10}$

步驟11：得到原發送的碼字為：

$c(x) = r(x) - e(x) =$

$x^4 + x^7 + x^{12} + x^{13} + x^{14} + x^{15} + x^{16}$

步驟12：解碼完成

用上述的解碼算法，我們成功地完成碼長分別為71,79,89,97,103,113六個平方剩餘碼的解碼[8-10]，其中每一個碼的解碼工作都用了超過100部電腦，平行處理各跑了幾個月才完成，工程不可不謂浩大，最後成果分為三篇，投稿發表在IEEE Transactions on Communications及Information Theory兩個學術刊物上。

§ Unified unknown syndrome representation method-Lagrange interpolation method

上一節的方法是將未知症狀子表為已知症狀子的函數，作法是先假設錯誤多項式中的錯誤數量，並根據這個數量，用論文[7]的方法得到未知症狀子的表示函數，所得到的函數與錯誤數量有關，因此，解碼過程是假設一個錯誤數量值，然後得到在這個錯誤數量下可用的未知症狀子表示函數，用這個函數作解碼。如果沒有結果，將錯誤數量加一，再得到未知症狀子表示函數，再作解碼，一直到所假設的錯誤數量超過糾錯能力。如果一直沒有解碼結果，表示該錯誤多項式為不可解錯誤，無法用代數解碼法來解。

對於一個有著多個錯誤的錯誤多項式，用上一節的方法來解碼的缺點是，要解許多次才能正確解出，這會降低解碼的效能，我們希望有只要一次解碼就能解出錯誤多項式的解碼法。為此，考慮一個能將未知症狀子表為已知症狀子的表示法，而且與錯誤多項式的錯誤數量無關，稱之為未知症狀子的一致表示法(unified unknown syndrome representation)。

這一小節，我們將針對第一型平方剩餘碼來求出未知症狀子的一致表示法。由於第一型平方剩餘碼的所有已知症狀子都是主要已知症狀子S_1的冪次方，而所有未知症狀子都是主要未知症狀子S_r的冪次方，因此只要將S_r表為S_1的函數，其他的已知、未知症狀子的值就可由S_1和S_r來求出。

根據可解錯誤多項式的性質，對於所有的可解錯誤多項式e(x)，它們的主要已知症狀子$S_1 = e(\beta)$的值都不一樣。令W為所有可解錯誤多項式的集合：

$W = \{x^{l_1} + \cdots + x^{l_i} | 0 \le l_1 < \cdots < l_i < n, 1 \le i \le t\}$

同時令Ω為所有主要已知症狀子的集合：$\Omega = \{e(\beta)|e(x) \in W\}$

則兩個集合有相同的元素個數，都是：

$$\binom{n}{1} + \cdots + \binom{n}{t}$$

令這個值為M，則Ω可表示為

$$\Omega = \{a_1, \ldots, a_M\}.$$

對所有 $i = 1, \ldots, M$ 若 $a_i = e(\beta) \in \Omega$，考慮 $b_i = e(\beta^r) \in E = GF(2^m)$。我們有$E$中$M$個相異元素 $a_1, \ldots, a_M$，以及E中M個元素 $b_1, \ldots, b_M$。如果E是實數集合，則由拉格朗日插值法(Lagrange interpolation formula)，可得到一個多項式 $L(x)$，使得

$$b_i = L(a_i), \forall i = 1, \ldots, M.$$

這個結果在有限體中也成立，而所需要的多項式如下：

$$L(x) = \sum_{i=1}^{M} b_i \prod_{\substack{k=1 \\ k \neq i}}^{M} \frac{x - a_k}{a_i - a_k}. \qquad (*)$$

式子(*)看起來是一個頗為龐大的多項式，不但項數可能多，係數也可能頗為複雜，我們用電腦計算了一些情形，卻發現了一些有趣的現象，這裡舉兩個例子：

範例7：考慮碼長為17的平方剩餘碼，其主要未知症狀子為S_3，現在用拉格朗日插值法(*)來求S_3的一致表示法：

由於最小距離d=5，能解兩個錯，可解錯誤多項式的集合W為：

$$W = \{x^0, \ldots, x^{16}\} \cup$$

$$\{x^0 + x^1, x^0 + x^2, \ldots, x^0 + x^{16}, \ldots, x^{15} + x^{16}\}$$

集合W中有 $\binom{17}{1} + \binom{17}{2} = 17 + 136 = 153$ 個元素，因此主要已知症狀子的集合Ω中也有M=153個元素：

$$\Omega = \{\beta^0, \ldots, \beta^{16}\} \cup \{\beta^0 + \beta^1, \beta^0 + \beta^2, \ldots,$$
$$x^0 + \beta^{16}, \ldots, \beta^{15} + \beta^{16}\} = \{a_1, \ldots, a_{153}\}$$

對所有 i =1,...,153，若 $a_i = e(\beta) \in \Omega$，考慮 $b_i = e(\beta^3) \in E = GF(2^m)$，用上述公式(*)，得到多項式 $L_{17}(x)$ 如下：

$$L_{17}(x) = x^{122} + x^{105} + x^{88} + x^{54} + x^3.$$

另外，考慮碼長為23的平方剩餘碼，其主要未知症狀子為S_5，模仿上面的做法，得到S_5的的一致表示法多項式 $L_{23}(x)$，如下：

$$L_{23}(x) = x^{1569} + x^{1546} + x^{1408} + x^{1316} + x^{1155} + x^{672} + x^{649} + x^{580} + x^{534} + x^{396} + x^{304} + x^{281} + x^{258} + x^{166} + x^{74} + x^{51} + x^{28}.$$

上述兩個例子中的多項式的項數都不算太多，都可以看成稀疏多項式(sparse polynomial)，同時它們還有一些共同現象，如下：

1.兩個多項式的非零項的係數都是1，亦即 $L_{17}(x), L_{23}(x) \in GF(2)[x]$

2.兩個多項式分別提出公因式 x^r 後，得到多項式的每一項的次數都是 n 的

倍數：

$$L_{17}(x) = x^3((x^{17})^7 + (x^{17})^6 + (x^{17})^5 + (x^{17})^3 + 1)$$

$$L_{23}(x) = x^5((x^{23})^{68} + (x^{23})^{67} + (x^{23})^{61} + (x^{23})^{57} + (x^{23})^{50} + (x^{23})^{29} + (x^{23})^{28} + (x^{23})^{25} + (x^{23})^{23} + (x^{23})^{17} + (x^{23})^{13} + (x^{23})^{12} + (x^{23})^{11} + (x^{23})^7 + (x^{23})^3 + (x^{23})^2 + (x^{23})^1)$$

上述現象並不是碼長$n=17$和$n=23$的特殊情形，而是所有第一型平方剩餘碼都會有的共同性質，我們證明了下面的結果：

定理：對於碼長為n的第一型平方剩餘碼，用拉格朗日插值法(*)來求未知症狀子S_r的一致表示法，所得到的多項式形式如下：

$$L_n(x) = x^r f(x^n), f(x) \in GF(2)[x]$$

因此，對所有的可解錯誤多項式$e(x) \in W$，有

$$S_r = e(\beta^r) = L(e(\beta)) = L(S_1).$$

有了這個結果，就可以根據它來發展第一型平方剩餘碼的新解碼算法，如下：

1.收到$r(\beta)$，計算主要已知症狀子$S_1 = r(\beta)$，如果S_1=0，表示$e(x) = 0$，不需要解碼，直接進入步驟7
如果$S_1 \neq 0$，表示$e(x) \neq 0$，進入下一步驟。

2.將症狀子S_1代入$L_n(x)$，而得到未知症狀子$S_r = L_n(S_1)$

3.用兩個主要症狀子S_1,S_r計算出$2t$個連續的症狀子：$S_1,...S_{2t}$

4.使用Berlekamp-Massey算法，得出錯誤位置多項式：$\sigma(x)$

5.使用錢氏搜尋法求得錯誤位置：$l_1, \dots, l_v$

6.得到錯誤多項式：$e(x) = x^{l_1} + \cdots + x^{l_v}$

7.得到原發送的碼字為：$c(x) = r(x) - e(x)$

8.解碼完成

用一個實際例子來說明上面的解碼算法：

範例8：考慮碼長為17的平方剩餘碼，假設碼字多項式為$c(x) = 0$，而錯誤多項式為$e(x) = x^3 + x^{10}$，因此接收多項式為$r(x) = c(x) + e(x) = x^3 + x^{10}$。使用上述的解碼算法來進行解碼：

步驟1：計算第一症狀子

$S_1 = r(\beta) = \beta^3 + \beta^{10} = \alpha^{38} \neq 0$，

步驟2：用$L_{17}(x) = x^{122} + x^{105} + x^{88} + x^{54} + x^3$來計算未知症狀子$S_3$：

$$S_3 = L_{17}(S_1) = L_{17}(\alpha^{38})$$

$$= (\alpha^{38})^3 + (\alpha^{38})^{54} + (\alpha^{38})^{88} + (\alpha^{38})^{105} + (\alpha^{38})^{122} = \alpha^{12}$$

步驟3：計算出$2t$=4個連續的症狀子：

S_1, S_2, S_3, S_4

$S_1 = \alpha^{38}$，

$S_2 = S_1^2 = (\alpha^{38})^2 = \alpha^{76}$，

$S_3 = \alpha^{12}$，

$S_4 = S_2^2 = (\alpha^{76})^2 = \alpha^{152}$，

步驟4：用Berlekamp-Massey演算法求得錯誤位置多項式 $\sigma(x)$ ：

$$\sigma(x) = 1 - \alpha^{38}x + \alpha^{195}x^2$$

步驟5：用錢氏搜尋法逐一將 $\beta^0, \ldots, \beta^{-16}$ 代入 $\sigma(x)$ 找其根：

$\sigma(\beta^0) = 1 - \alpha^{38}(\beta^0) + \alpha^{195}(\beta^0)^2 = \alpha^{174} \neq 0$，
$\sigma(\beta^{-1}) = 1 - \alpha^{38}(\beta^{-1}) + \alpha^{195}(\beta^{-1})^2 = \alpha^{210} \neq 0$，
$\sigma(\beta^{-2}) = 1 - \alpha^{38}(\beta^{-2}) + \alpha^{195}(\beta^{-2})^2 = \alpha^{42} \neq 0$，
$\sigma(\beta^{-3}) = 1 - \alpha^{38}(\beta^{-3}) + \alpha^{195}(\beta^{-3})^2 = 0 \Rightarrow l_1 = 3$
$\sigma(\beta^{-4}) = 1 - \alpha^{38}(\beta^{-4}) + \alpha^{195}(\beta^{-4})^2 = \alpha^{80} \neq 0$
$\sigma(\beta^{-5}) = 1 - \alpha^{38}(\beta^{-5}) + \alpha^{195}(\beta^{-5})^2 = \alpha^{235} \neq 0$，
$\sigma(\beta^{-6}) = 1 - \alpha^{38}(\beta^{-6}) + \alpha^{195}(\beta^{-6})^2 = \alpha^{11} \neq 0$，
$\sigma(\beta^{-7}) = 1 - \alpha^{38}(\beta^{-7}) + \alpha^{195}(\beta^{-7})^2 = \alpha^{103} \neq 0$，
$\sigma(\beta^{-8}) = 1 - \alpha^{38}(\beta^{-8}) + \alpha^{195}(\beta^{-8})^2 = \alpha^{190} \neq 0$，
$\sigma(\beta^{-9}) = 1 - \alpha^{38}(\beta^{-9}) + \alpha^{195}(\beta^{-9})^2 = \alpha^{5} \neq 0$，
$\sigma(\beta^{-10}) = 1 - \alpha^{38}(\beta^{-10}) + \alpha^{195}(\beta^{-10})^2 = 0 \Rightarrow l_2 = 10$
$\sigma(\beta^{-11}) = 1 - \alpha^{38}(\beta^{-11}) + \alpha^{195}(\beta^{-11})^2 = \alpha^{162} \neq 0$，
$\sigma(\beta^{-12}) = 1 - \alpha^{38}(\beta^{-12}) + \alpha^{195}(\beta^{-12})^2 = \alpha^{45} \neq 0$，
$\sigma(\beta^{-13}) = 1 - \alpha^{38}(\beta^{-13}) + \alpha^{195}(\beta^{-13})^2 = \alpha^{234} \neq 0$，
$\sigma(\beta^{-14}) = 1 - \alpha^{38}(\beta^{-14}) + \alpha^{195}(\beta^{-14})^2 = \alpha^{134} \neq 0$，
$\sigma(\beta^{-15}) = 1 - \alpha^{38}(\beta^{-15}) + \alpha^{195}(\beta^{-15})^2 = \alpha^{68} \neq 0$，
$\sigma(\beta^{-16}) = 1 - \alpha^{38}(\beta^{-16}) + \alpha^{195}(\beta^{-16})^2 = \alpha^{104} \neq 0$，

由以上結果得知，β^{-3} 和 β^{-10} 為 $\sigma(x)$ 的根，因此錯誤位置 $l_1 = 3$ ， $l_2 = 10$

步驟6：錯誤多項式為 $e(x) = x^3 + x^{10}$

步驟7：碼字多項式為 $c(x) = r(x) - e(x) = (x^3 + x^{10}) - (x^3 + x^{10}) = 0$

步驟8：解碼完成。

另外，再附一個碼長23的例子：

訊息多項式： $a(x) = x^9 + x^{10} + x^{11}$

碼多項式： $c(x) = x^9 + x^{12} + x^{14} + x^{16} + x^{19} + x^{21} + x^{22}$

錯誤多項式： $e(x) = x^4 + x^{13} + x^{21}$

接收多項式：

$r(x) = x^4 + x^9 + x^{12} + x^{13} + x^{14} + x^{16} + x^{19} + x^{22}$

症狀子： $S_1 = r(\beta) = \alpha^{968}$

$S_2 = S_1^2 = (\alpha^{968})^2 = \alpha^{1936}$

$S_3 = S_2^{128} = \alpha^{121}$

$S_4 = S_2^2 = (\alpha^{1936})^2 = \alpha^{1825}$

$S_5 = L_{23}(\alpha^{968}) = \alpha^{669}$

$S_6 = S_3^2 = \alpha^{242}$

錯誤位置多項式：

$\sigma(x) = 1 - \alpha^{968}x + \alpha^{226}x^2 - \alpha^{1335}x^3$

根： $x = \alpha^{-356} = \beta^{-4}, x = \alpha^{-1157} = \beta^{-13}, x = \alpha^{-1869} = \beta^{-21}$

錯誤位置： $l_1 = 4, l_2 = 13, l_3 = 21$

結束語

平方剩餘碼在1958年被提出來，著名編碼學者Berlekamp在他的書中提到，平方剩餘碼是一種好的碼，只是解碼是困難的，也因此才在32年後，由Reed教授提出Golay碼外第一個平方剩餘碼的解碼方法，此後其他的平方

剩餘碼的解碼算法分別由南加大以及義守大學的團隊提出，雖然我們只處理到碼長113，然而相同的方法可以繼續作下去，只是對於更大的碼長，平方剩餘碼也不再繼續保有較大最小距離的優勢，實用價值就沒有那麼大。

另外，建立在插值法而發展出來的一次型解碼，本文提出的結果只適用於第一型平方剩餘碼；對於第二型平方剩餘碼，我們也發展了一個有限體上多變數插值法(multivariate interpolation formula over finite field)，可用來求得未知症狀子的一致表示法，然後用Berlekamp-Massey算法來解碼，這個方法不只是可以用來解第二型平方剩餘碼，還可以用來解一般的循環碼，目前論文正在準備中，尚未正式發表。

參考文獻

[1]I. S. Reed and G. Solomon (1960), Polynomial Codes Over Certain Finite Fields, *SIAM Journal of Applied Math.*, vol. 8, pp. 300-304.

[2]T. Kasami (1964), A Decoding Procedure for Multiple-Error-Correcting Cyclic Codes, *IEEE Trans. Inform. Theory*, vol. IT-10, no. 2, pp. 134–138.

[3]M. Elia (1987), Algebraic decoding of the (23, 12, 7) Golay code, *IEEE Trans. Inform. Theory*, vol. 33, pp. 150-151.

[4]I. S. Reed, X. Yin, and T. K. Truong (1990), Algebraic decoding of the (32, 16, 8) quadratic residue code, *IEEE Trans. Inform. Theory*, vol. 36, pp. 876-880.

[5]I. S. Reed, T. K. Truong, X. Chen, and X. Yin (1992), The algebraic decoding of the (41, 21, 9) quadratic residue code, *IEEE Trans. Inform. Theory*, vol. 38, pp.974-985.

[6]X. Chen, I. S. Reed, and T. K. Truong (1994), Decoding the (73, 37, 13) quadratic residue code, *Proc.IEE*, vol. 141, pp. 253-258.

[7]R. He, I. S. Reed, T. K. Truong, and X. Chen (2001), Decoding the (47, 24, 11) quadratic residue code, *IEEE Trans. Inform. Theory*, vol. 47, pp. 1181–1186.

[8]Y. Chang, T. K. Truong, I. S. Reed, H. Y. Cheng, and C. D. Lee (2003), Algebraic decoding of (71, 36, 11), (79, 40, 15), and (97, 49, 15) quadratic residue codes, *IEEE Trans. Commun.*,vol. 51, no. 9, pp. 1463–1473.

[9]T. K. Truong, Y. Chang, Y. H. Chen, and C. D. Lee (2005), Algebraic decoding of (103, 52, 19) and (113, 57, 15) quadratic residue codes, *IEEE Trans. Commun.*, vol. 53, no. 5, pp. 749–754.

[10]T.-K. Truong, P.-Y., Shih, W.-K. Su, C.D. Lee, and Y. Chang (2008), Algebraic decoding of the (89, 45, 17) quadratic residue code, *IEEE Trans. Information Theory*, vol. 54, no .11, pp. 5005–5011.

附表 1：平方剩餘碼參數表

n	k	d		n	k	d		n	k	d
7	4	3*		73	37	13		137	69	21
17	9	5*		79	40	15*		151	76	19
23	12	7*		89	45	17*		167	84	23
31	16	7*		97	49	15		191	96	27
41	21	9*		103	52	19*		193	97	27
47	24	11*		113	57	15		199	100	31*
71	36	11		127	64	19				

表：不同數量錯誤時的牛頓等式及求得的錯誤位置多項式

錯誤數量	牛頓等式	錯誤位置多項式
v=1	$S_1 + \sigma_1 = 0$	$\sigma(x) = 1 + S_1 x$
v=2	$S_1 + \sigma_1 = 0$ $S_3 + \sigma_1 S_2 + \sigma_2 S_1 = 0$	$\sigma(x) = 1 + S_1 x + ((S_3 + {S_1}^3)/S_1)x^2$

錯誤數量	牛頓等式	錯誤位置多項式
v=3	$S_1 + \sigma_1 = 0$ $S_3 + \sigma_1 S_2 + \sigma_2 S_1 + \sigma_3 = 0$ $S_5 + \sigma_1 S_4 + \sigma_2 S_3 + \sigma_3 S_2 = 0$ $S_7 + \sigma_1 S_6 + \sigma_2 S_5 + \sigma_3 S_4 = 0$ $S_9 + \sigma_1 S_8 + \sigma_2 S_7 + \sigma_3 S_6 = 0$	$\sigma(x) = 1 + S_1 x + \left(S_1{}^2 + D^{1/3}\right)x^2 + (S_3 + S_1 D^{1/3})x^3$ $D = (S_3 + S_1{}^3)^2 + (S_9 + S_1{}^9)/(S_3 + S_1{}^3)$

BACK

義大醫院、義守大學近期活動

義大醫院

新型流感之防治

主講人：義大醫院感染科鍾幸君副主任

日期：　105年4月2日(六) 7:30-8:30a.m.

地點：　義大癌治療醫院六樓會議廳

增生療法(prolotherapy)之介紹--高濃度葡萄糖局部注射治療慢性疼痛新進展

主講人：義大醫院復健科—林純如醫師

日期：　105年4月9日(六) 7:30-8:30a.m.

地點：　義大癌治療醫院六樓會議廳

臨床抗生素使用原則

主講人：義大醫院感管實驗科—賴重旭主任

日期：　105年5月7日(六) 7:30-8:30a.m.

地點：　義大癌治療醫院六樓會議廳

Translational study - A boost to human health of well-being- use Chinese hurbal formula research as an example

主講人：義大醫院感管婦產部—黃瑟德醫師

日期：　105年5月9日(六) 7:30-8:30a.m.

地點：　義大癌治療醫院六樓會議廳

手部衛生推廣

主講人：義大醫院感管感染科—鍾幸君副主任

日期：　105年6月23日(四) 7:30-8:30a.m.

地點：　義大癌治療醫院六樓會議廳

義守大學

2016年第七屆全國日語俳句大賽

主講人：義守大學應用日語學系—花城可裕講師

日期：　105年2月28日(日)～5月31日(二)

地點：　義守大學應日系

瘤岩、肛腸病

主講人：陳光偉中醫診所所長—陳光偉所長

日期：　105年4月21日(四)

地點：　義守大學醫學院區C1035室

專題演講

主講人：日本高知新聞社編輯—阿萬美香小姐

日期：　105年4月27日(三)

地點：　義守大學應日系

乳房疾病、癭病

主講人：財團法人佛教慈濟綜合醫院一般外科以及財團法人彰化基督教醫院體系乳房中心—蘇進成主任

日期：　105年4月28日(四)

地點：　義守大學醫學院區C1035室

臨床藥理特別演講

主講人：臺大醫院外科部主治醫師—李伯皇醫師

日期：　105年5月5日(四)

地點：　義守大學醫學院區C1033室

電機產業與就業趨勢發展—半導體產業分析說明

主講人：臺大醫院外科部主治醫師—李伯皇醫師

日期：　105年5月18日(三)

地點：　義守大學科技大樓3801教室

104 學年度南區大專院校碩士班聯合發表大會

主講人：義守大學應用日語學系—泰田伊知朗副教授

日期：　105年5月21日(六)

地點：　義守大學應日系

中醫診斷學臨床技能考試

主講人：義守大學學士後中醫學系—李長殷助理教授

日期：　105年6月15日(三)

地點：　義守大學醫學院臨床技能教室

電機產業與就業趨勢發展—產業升級，創新研發

主講人：工業技術研究院—張守芳小姐/周錫昌先生

日期：　105年6月

地點：　義守大學科技大樓3801教室

BACK

科技部消息

＊公開徵求歐盟水資源於農林及淡水產養殖業之永續管理計畫-WaterWorks2015。

一、科技部參與歐盟WaterWorks2015 計畫，與歐洲各國同步公開徵求計畫書，細節 請參閱Water JPI 網站- http://www.waterjpi.eu/)英文版之「Call-Announcement-All-In-One」檔案，本次公開徵求之主題為:Sustainable management of water resources in agriculture, forestry and freshwater aquaculture sectors.

二、Pre-Proposal計畫截止日: 2016年4月19日

三、詳細細節請參閱附件說明檔及歐方WATER JPI網站上公告之文件及線上申請程序。

四、訊息相關網址：https://goo.gl/6m8mir

五、計畫截止日：105年4月19日

＊公開徵求105年度「科技部補助任務導向型團隊赴國外研習計畫」，至105年4月29日申請截止。

一、 本(105)年度關鍵性之科技及人文社會研究項目計有15項，國外研習機構在新增或刪除後計有66所，可前往合作及研習之實驗室達150間。

二、 105年度之作業時程如下：

1. 計畫申請：105年1月18日起至105年4月29日止(以系統送出為憑)；申請機構函送申請名冊到部請於105年5月4日前(以公文發文日為憑)。
2. 公告結果日期：105年7月31日前。
3. 計畫執行日期：105年9月1日至106年8月31日(第二年期計畫順延一年)。
4. 國外研習機構參考意見：申請人(計畫主持人)應提醒擬前往之國外研習機構指導人直接將意見於105年5月6日前寄達科技部科教國合司業務承辦人(cttao@most.gov.tw)。

三、年度關鍵領域及國外研習機構請參閱附檔，另本案作業要點及相關文件請至科技部科教國合司相關網頁下(https://goo.gl/HbSNjk)參考。

四、訊息相關網址：https://goo.gl/PUh4UD

五、計畫截止日：105年4月29日

產學消息

＊經濟部技術處「鼓勵中小企業開發新技術計畫」（SBIR）方案

一、SBIR計畫就是「小型企業創新研發計畫（Small Business Innovation Research）」，它是經濟部為鼓勵國內中小企業加強創新技術或產品的研發，依據「經濟部促進企業開發產業技術辦法」所訂定的計畫，期望能以此協助國內中小企業創新研發，加速提升中小企業之產業競爭力，以迎接面臨之挑戰。

二、申請資格：依公司法設立之中小企業

三、受理期間：計畫為政府持續推動與支持之計畫，廠商可隨時提出申請，並無特定的申請截止日期

四、相關聯結：http://goo.gl/TqaNG0

＊經濟部工業局「主導性新產品開發輔導計畫」

一、政府為鼓勵民營事業研究開發主導性新產品，發展高科技之新興產業，提升技術層次，調整工業結構，提高國際競爭力，促進經濟成長，依據行政院「加速製造業升級及投資方案」第三項措施「加速資本及技術密集工業之發展」，訂定「主導性新產品開發輔導辦法」，以提供研究開發補助經費方式，鼓勵國內新興高科技工業具有研究發展潛力之廠商，參與本項輔導計畫。

二、申請資格：依公司法設立之公司(詳細資格條件請參閱網站)

三、受理期間：計畫為政府持續推動與支持之計畫，廠商可隨時提出申請，並無特定的申請截止日期

四、相關聯結：http://outstanding.itnet.org.tw/

＊經濟部技術處「A+企業創新專案」相關計畫

一、為鼓勵企業從事技術創新及應用研究，建立研發能量與制度，經濟部開放企業界申請「業界科專」計畫，藉以政府的部分經費補助，降低企業研發創新之風險與成本，且研發成果歸廠商所有，以積極鼓勵業者投入產業技術研發工作，在業界提出申請及執行計畫過程中，輔導業界建立研發管理制度、強化研發組織、培育及運用科技人才、誘發廠商自主研發投入與後續投資，並促進產、學、研之間的交流與合作，健全業界整體發展能力，達到政府「藏技於民」的美意。

二、申請資格：依公司法設立之本公司或從事與創新服務研究發展活動相關具稅籍登記之事務所及醫療法人、財務健全、其專業團隊具從事提供 知識之創造、流通或加值之工作經驗且有實績者，均可提出計畫申請。

三、受理期間：計畫為政府持續推動與支持之計畫，廠商可隨時提出申請，並無特定的申請截止日期

四、相關聯結：http://aiip.tdp.org.tw/index.php

＊經濟部工業局「協助傳統產業技術開發計畫」（CITD）

一、為落實照顧傳統產業政策，經濟部工業局度積極透過「協助傳統產業技術開發計畫」，將近投入新台幣4億元，協助並鼓勵傳統產業進行新產品開發、產品設計及聯合開發，預計將嘉惠290家以上傳統產業業者，提升其競爭力。

二、申請資格：須為民間傳統產業業者(詳細資格條件請參閱網站)

三、受理期間：每年兩次，約為12月～隔年1月、4月～5月

四、相關聯結：http://goo.gl/hWQ1Hj

＊高雄市政府「地方產業創新研發推動計畫」（高雄市政府地方型SBIR）

一、為協助各直轄市、縣(市)政府，經濟部特配合匡列相對經費，俾利各直轄市、縣(市)政府擁有加倍之經費得以辦理地方特色產業創新研發計畫之推動，帶動中小企業積極投入地方特色產業之研發，而提升具地方特色產業聚落創新研發之能量，以鼓勵中小企業創新研發之政策得以在地方紮根。基此，特規劃由各直轄市、縣(市)政府辦理「地方產業創新研發推動計畫」（地方型SBIR）。

二、申請資格：依公司法設立之中小企業，且其本公司住

所設於高雄市並取得高雄市政府核發之營利事業登記證者；或依法取得高雄市政府核發工廠登記證之工廠。(詳細資格條件請參閱網站)

三、受理期間：約為每年4～6月（依網站公告為主）

四、相關聯結：http://96kuas.kcg.gov.tw/sbir/main.php

＊屏東縣政府「地方產業創新研發推動計畫」（屏東縣政府地方型SBIR)

一、為協助各直轄市、縣(市)政府，經濟部特配合匡列相對經費，俾利各直轄市、縣(市)政府擁有加倍之經費得以辦理地方特色產業創新研發計畫之推動，帶動中小企業積極投入地方特色產業之研發，而提升具地方特色產業聚落創新研發之能量，以鼓勵中小企業創新研發之政策得以在地方紮根。基此，特規劃由各直轄市、縣(市)政府辦理「地方產業創新研發推動計畫」（地方型SBIR）。

二、申請資格：依公司法設立之中小企業，且其本公司住所設於高雄市並取得高雄市政府核發之營利事業登記證者；或依法取得高雄市政府核發工廠登記證之工廠。(詳細資格條件請參閱網站)

三、受理期間：約為每年4～6月（依網站公告為主）

四、相關聯結：http://www.ptsbir.org.tw/

＊科技部「補助產學合作研究計畫」

一、整併原有的大產學、小產學及數位產學相關補助要點，並建構產業需求導向之產學合作模式，以整合運用研發資源，發揮大學及研究機構之研發力量，以期能透過產學的團隊合作與相互回饋的機制，提升國內科技研發的競爭力。分為「先導型」、「應用型」及「開發型」計畫。

二、申請資格：

●申請機構（以下稱計畫執行機構）：係指公私立大專校院、公立研究機構及經本會認可之財團法人學術研究機構。

●合作企業：係指依我國相關法律設立之獨資事業、合夥事業及公司，或以營利為目的，依照外國法律組織登記，並經中華民國政府認許，在中華民國境內營業之公司，並以全程參與本會產學合作研究計畫為原則。

三、受理期間：

●先導型產學合作計畫，申請日期約為每年2月。

●應用型產學合作計畫，申請日期約為2月及5月。

●開發型產學合作計畫，申請日期約為2月、5月及10月。

四、相關聯結：https://goo.gl/L6NdjM

＊教育部「大專畢業生創業服務計畫」

一、為縮短大專校院學生畢業與就業間連結之平台落差，建立產學合作創業就業機制，結合各部會產業發展之資源，引導大專校院學生就業機會，實施大專畢業生創業服務計畫。

二、申請資格：

- 設有育成單位之公私立大專校院。
- 創業團隊由各大專校院畢業生至少三人組成，其中應有三分之二以上成員為近三學年度(應屆及前二學年度)畢業生，每人限參與一組團隊，且各團隊之代表人應為近三學年度畢業者。(團隊及團員未曾接受本計畫之補助)

三、受理期間：每年5～6月

四、相關聯結：http://ustart.yda.gov.tw/bin/home.php

BACK

義守大學 研究發展處

84001 高雄市大樹區學城路一段1號

電話：07-657-7711

傳真：07-657-7471

Mail : research@isu.edu.tw

義大醫院 醫學研究部醫學教育部

82445 高雄市燕巢區角宿里義大路1號

電話：07-615-0011

傳真：07-615-5352

Mail : ed103390@edah.org.tw
ed100075@edah.org.tw

發行人： 蕭介夫 校長 / 杜元坤 院長

總編輯： 林麗娟 副校長 / 楊生滿 副院長

陳立軒 研發長 / 沈德村 行政長

編輯部： 張慧柔組長、朱堃誠組長、許世宏先生 / 陳素婷課長、李雅純小姐、陳麗芬小姐

BACK