數位訊息，使命必達—

錯誤訊息的偵測與修正

為什麼條碼機可以正確地讀出你購買的商品價錢？為什麼稍稍刮損的音樂CD仍可播放？數位訊息中暗藏著什麼祕密，且讓我們來一探究竟。

賴昭正

筆者在《科學月刊》第468期（2008年12月號）的〈GPS的定位數學〉裡提到，衛星發射信號的功率在50瓦左右，我們也談到衛星的飛行高度大約在2.5萬公里左右。因訊號的強度與距離的平方成反比，故其到達地球表面的訊號強度大約只有1.3×10^{-17}瓦／平方公分，是非常弱的。相較之下，一般家用無線網路的功率大約在0.1瓦，其有效距離在100公尺內，其強度尚有1×10^{-9}瓦／平方公分。因此GPS的接收機應比家用無線網路的接收機敏感多了！

即使如此，我們還是很難想像，它能完全無誤地接收訊息，更何況衛星發射器本身及傳遞的過程中均可能產生錯誤訊息。GPS是用來定位的，些許的錯誤訊息很可能造成「差之毫釐，失之千里」！例如某顆衛星在台北的上空，但一字之差，接收機以為它在台南上空，計算後可能告訴你，你即將掉進台灣海峽了！如何解決此類問題正是本文所要探討的。

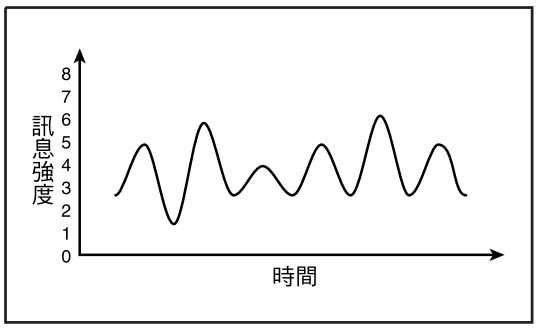
類比 vs.數位

要避免像上述掉進台灣海峽的烏龍事件發生，接收機的首要功能應是能偵測到訊息的錯誤。在現今所謂的資訊時代，具備此一功能的設備，事實上已是日常生活中不可或缺的工具，只是大部分的人都沒有注意到而已。例如百貨公司所用的條碼機就有此一功能，相信許多讀者都有這個經驗：第一次掃描若發生錯誤，條碼機就會告訴服務員要重新掃描一次。可是條碼機如何知道它讀的資料有誤呢？

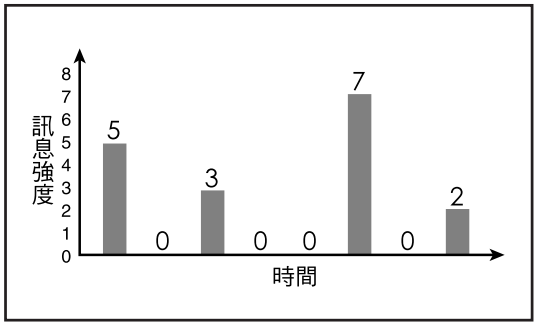
很顯然地，錯誤訊息的偵測一定是存在訊息本身內的。在討論訊息本身如何「儲存」偵測錯誤的能力之前，我們得先在這裡談一下訊息結構的種類。訊息的結構與傳播可分為類比（analog）及數位（digital）兩種。早期的訊息幾乎全是類比，類比的訊息是以波動的連續變化來儲存與傳遞（圖一）；但隨著微電腦及積體電路的不斷改進，數位訊息的使用已越來越廣泛。數位訊息是以數碼的形式來儲存與傳遞訊息（圖二），如果原訊息是類比訊息，則須先將它數位化（digitalize）。數位訊息的最大優勢是可輕易且正確地複製及處理，以及本文所要談到的：可以輕易地偵測到訊息本身的錯誤並修正它。

錯誤訊息的偵測

如果圖一中的波形受干擾，發生不怎麼



圖一：類比訊息，以波動的連續變化儲存與傳遞。



圖二：數位訊息，以數碼來儲存與傳遞。

大的變形，我們無法判斷到底是因為「原來的信號就是如此」或是「錯誤」所致。但如果是圖二中的信號「50300702」受到少許的干擾，如5的高度變成5.2，則因為訊息只有整數的，故我們可以毫無困難地知道（偵測到）5.2是錯誤的，應該修正為5才對。這正是一種錯誤訊息的偵測與修正，相信是大家均早已知曉的數碼傳遞優點；但因其邏輯簡單，沒什麼研究可做（申請不到任何研究經費的），因此一般都不把它歸入「錯誤訊息的偵測與修正」。

聰明的讀者也許立即想到：如果干擾較大點，變成5.6呢？不錯，那我們的接收器只好把它當成6了。沒問題，雖然產生了「這麼大」的錯誤，但我們還是有辦法知道接收的訊息錯了，例如我們「規定」每8個數目的總和必須是奇數（5＋0＋3＋0＋0＋7＋0＋2＝17），則第一個數目誤接收為6時，其總和便為偶數。錯了，請服務員再掃描一次吧！

如果干擾更大，5變成7怎麼辦呢？上面的奇數策略當然就不管用了。但要解決此一難題，事實上很簡單：我們可以「規定」8個數目的總和必須是9的倍數就可以了。當然，在條碼的運用上，這種「規定」很容易做得到。但如果應用到其他由類比數位化成的訊息時，就很難加以這樣「規定」（限制）了。解決此一問題的方法，事實上正是所有偵測訊息錯誤所採用的方法——在訊息本身外加上其他「冗位」（redundancy）的資料。例如在前面所用的8位數資訊後，我們可以再加一位數，成為9位數的字碼（codeword）。這樣我們就不須要「限制」前面的8位數（它們可以是由任何數字組合成），仍然可以達到字碼必須是9的倍數之要求（圖三）。請讀者在此特別注意：這冗位的數字不是隨便給的，而是由資訊本身（更正確地說，應是字碼本身）「計算」得來的——字碼必須是9的倍數！

圖三：在這串訊息中，前8位數為有用的資訊，最後一位則是「冗位」，總共是9位數的字碼。

利用此一「編碼法」，我們可以很容易地偵測出字碼錯誤（不是9的倍數），但卻不知錯誤在那裡。這用在條碼等訊息傳輸上不是大問題——只要使用者（例如服務員）再重讀一次即可〔註一〕。但在很多的實用方面卻會構成大問題；例如在聽音樂CD時，我們不能叫聽者暫停，讓CD播放機重讀一下錯誤的訊息〔註二〕。因此在許多實用上，我們不只要有偵測錯誤訊息的能力，還須具備即時修正的能力，底下我們就來談談錯誤訊息的修正。

錯誤訊息的修正

在前面的例子裡（字碼必須是 9 的倍數），我們只要將字碼連續傳遞兩次，則我們不但能偵側到訊息的錯誤，還可以同時完成修正。例如我們收到的訊息是：

503007021 505007021

則我們不但知道訊息有誤，還知道第三位數應是 3 而不是 5（因第三位數不同，且總和應是9的倍數），這結果看來非常好，但仔細一想，未免太浪費「資源」了：本來只要傳遞 8 位數的訊息，現在卻須傳遞 18 位數。這「資源」在訊息傳播上稱為頻寬（bandwidth）。頻寬就像土地一樣，隨著人口的增加及生活水準的不斷提升，正是寸土寸金浪費不得的。

相信不少讀者早就想問：如果有兩位數字同時發生錯誤怎麼辦？答案很簡單：沒辦法，此編碼法不能用於修正同時含兩個（或兩個以上）錯誤的訊息。那怎麼辦呢？其解決方法有二：其一是尋根究底改進訊息的產生與傳遞，以及接收的機構，來降低錯誤的發生率到編碼法可以輕鬆完成任務的地步；其二則是設計「更好」的編碼方法，本文後面將會談論到。

在這裡順便一提，所有錯誤訊息的偵測及修正法均是採用在原訊息中增加「冗位」的資料來完成的。這看來在資訊的儲存上似乎是個浪費，但如果仔細分析，就會知道這結論並不完全正確。例如在錄音帶的系統中，因有偵測及修正錯誤的能力，我們可以減低對訊號雜訊比（signal to noise ratio）的要求，而使用較狹窄的錄音帶。

到此為止，筆者所談的錯誤偵測與修正法，均可用直覺來推斷，缺少理論的基礎，但筆者相信已將其原理用白話清楚地表達出來。實用的編碼方法很多，也都有數學基礎，但那數學卻不是一般高中或大學所涉及的〔註三〕，因此我們在此不擬討論其推理，而僅說明結果。底下就是個無法用「直覺」想出來的例子——音樂CD編碼的基本原理，如果不是數學家早有研究，相信索尼（Sony）及飛利浦（Philips）不會那麼快就發展出今日的 CD 標準。

漢明碼

為了能夠清楚地說明漢明碼（Hamming codes），我們將以一個由7個二進位數組成的字碼來做為例子：

1010 0001
資訊 檢測

前面 4 位數是（有用的）資訊，而後面的 3 位數則是我們前面所談到之「冗位」資料，在錯誤訊息的偵測與修正上，一般稱為「同位位元」（parity bit）。用 3 位數來檢測與修正 4 位元的資訊，好像也比前面的 10：8之頻寬浪費好不了多少。不錯，但這是為了說明方便，所以才採用 3 位元來檢視。如果我們採用4位元來檢測，則有用的資料長度可達 11 位元；用 5 位元來檢測與修正，有用的資料長度可高達 26 位元！

如前所述，同位位元並不是隨便加進去的，必須依一定規則計算出來。如果我們用 b_1 、 b_2 、 b_3 及 b_4 來代表前面的資訊，則後面 3 位檢測位元 p_1 、 p_2 及 p_3 依數學分析將分別為：

$$p_1 = b_1 + b_2 + b_3$$
$$p_2 = b_1 + b_3 + b_4$$
$$p_3 = b_2 + b_3 + b_4$$

上面的「＋」為二進位運算中的「互斥或（exclusive OR）」：

$1 + 1 = 0$

$1 + 0 = 1$

$0 + 1 = 1$

$0 + 0 = 0$

所以如果資訊為 1010 ，我們得：

$p_1 = 1 + 0 + 1 = 0$

$p_2 = 1 + 1 + 0 = 0$

$p_3 = 0 + 1 + 0 = 1$

將這3位檢測位元加到原資訊後面，我們便得字碼：

1 0 1 0 0 0 1

如果我們收到的字碼為（$b_1b_2b_3b_4p_1p_2p_3$），我們如何偵測及修正錯誤呢？我們由所接收到的字碼計算出 3 個「接收檢測位元」：

$Q_1 = b_1 + b_2 + b_3 + p_1$

$Q_2 = b_1 + b_3 + b_4 + p_2$

$Q_3 = b_2 + b_3 + b_4 + p_3$

如果接收到之字碼沒錯，則$Q_1 = Q_2 = Q_3 = 0$；如果僅有一位位元有錯（此一漢明碼不能同時偵測兩個或以上之錯誤），則其中至少有一Q不為零，我們可由（Q_1, Q_2, Q_3）之值推斷錯誤所在處如下〔註四〕：

（1,1,0）→ b_1

（1,0,1）→ b_2

（1,1,1）→ b_3

（0,1,1）→ b_4

（1,0,0）→ p_1

（0,1,0）→ p_2

（0,0,1）→ p_3

然後將錯誤處之值0→1或1→0 即可。例如原字碼為 1010001 ，但我們收到為 1110001 ，則我們得：

$Q_1 = 1 + 1 + 1 + 0 = 1$

$Q_2 = 1 + 1 + 0 + 0 = 0$

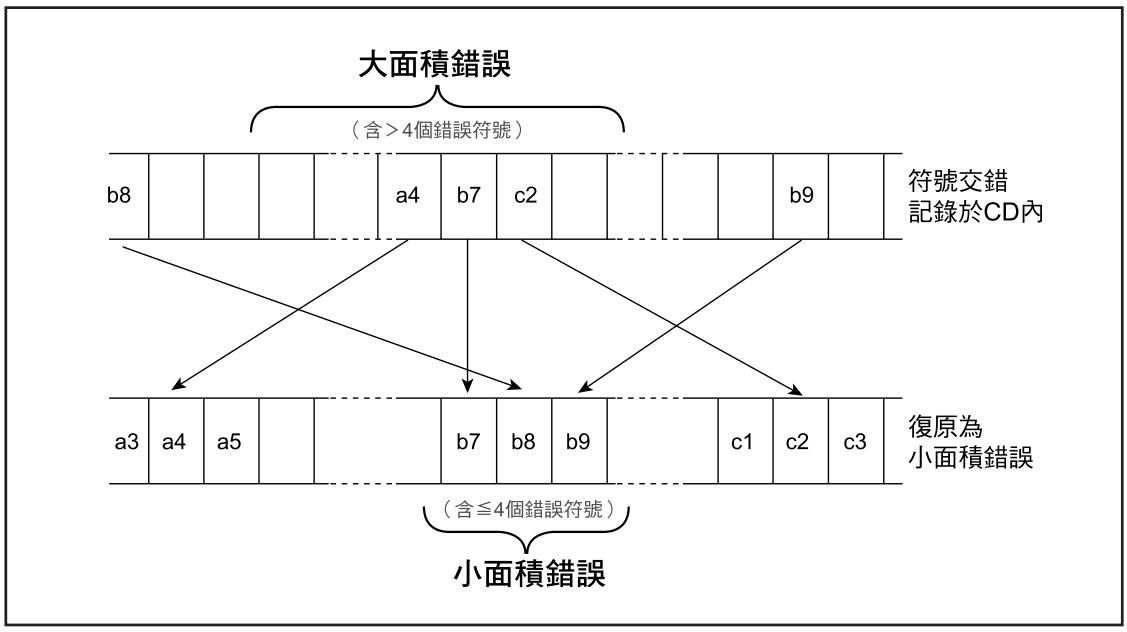
$Q_3 = 1 + 1 + 0 + 1 = 1$

即（Q_1, Q_2, Q_3）=（1,0,1），所以我們可以得知 b_2 是錯誤的！這些計算看來雖然不怎麼複雜，不過似乎很繁瑣；但其運算方式是計算機設計的基本邏輯，因此可以利用微電腦線路，完全自動化地偵測及修正接收到的資訊。

里德－所羅門碼

在音樂CD中所用的錯誤偵測原理雖然與上面的例子相似，但當然要比它複雜多了。我們上面例子裡的每個二進位位元，在音樂 CD 裡則是由 8 位位元組成的「符號」（symbol）；檢測位元也是由符號組成的。它的字碼由 24 個資料符號及 8 個檢測符號組成（共 32 個符號），可以同時偵測及修正 4 個資料符號。此一「編碼法」是里德（Irving Reed）及所羅門（Gustave Solomon）於 1960 年，在美國麻省理工學院林肯實驗室發展出來的，稱為里德－所羅門碼（Reed-Solomon codes ，簡稱 RS 碼）。

為了能修正「大面積」錯誤（burst error），此編碼法更將原來的一連串符號（包括檢測符號）交錯記錄於音樂CD內，這樣原來 RS 碼無法修正的大面積錯誤（大於 4 個資料符號）在復原時就被「打散」成許多RS碼可以處理的小面積（等於或小於4個資料符號）錯誤（圖四）。在音樂 CD 的編碼上，此一做法稱為「交叉插入里德—所羅門碼（cross interleave Reed-Solomon code，簡稱 CIRC）」。這說明了為什麼在音樂 CD 上刮上一道（請勿輕易嘗試），有時還是不會失真的原因。當然，要產生原來音樂前，得先將交錯復原後再解碼。



圖四：將原來的符號交錯記錄於音樂 CD 內，把原來 RS 碼無法修正的大面積錯誤打散，成了許多可以處理的小面積錯誤。

結 語

隨著微電腦及積體電路的不斷改進，數位訊息的使用已越來越廣泛：從微電腦本身到MP3 、音樂CD 、 DVD影碟機、電影、錄影機、照相機、無線電廣播、電視、電台……等等。數位訊息最大的優勢是處理（如修改）容易、可輕易且完美地複製、以及可以「很容易地」偵測到其傳遞錯誤的訊息並修正之。本文不用數學，簡單地介紹了數位訊息傳遞錯誤的偵測與修正的基本原理：在原訊息中增加「多餘」的「同位位元」來達成（例如音樂CD裡就多加了三分之一的同位位元）。雖然我們未能深入地討論其數學，但希望讀者還是能因本文而了解到，看似簡單的日用品後面，事實上是暗藏了常被視為無用之「純」數學的研究成果！

註一：電腦的記憶體就是使用此一原理（9 位元，其中有一位元是屬於「冗位」的）；但因電源及其設計越來越穩定，不少個人電腦都已開始採用不須「冗位」位元的記憶結構（買記憶體時應注意）。

註二：隨身聽音樂CD播放機因隨時在動的關係，其錯誤訊息出現的頻率遠超過家用音樂CD播放機，因此必須常常利用重讀來解決錯誤的問題，所以較貴的CD隨身聽機都有所謂的「抗震」功能。它們是先將資料儲存於緩衝區，然後依序播放。緩衝區越大，抗震的能力當然也越大。緩衝區使得它們有時間（不須暫停）去重讀錯誤的資料。

註三：所用的數學為抽象代數學（abstract algebra）中的場（field）論。我們所熟知的一個例子是：所有的實數及其運作（加減及乘除）規則構成了一個抽象代數中的「（無限）場」（因具有無限的實數）。

註四：如果讀者對排列組合有興趣，可以輕易算出Q_i不全為0的情形共有7種，這正是7位元資訊單一錯誤的可能情形！利用此一分析，讀者也可了解為什麼我們在文中說：「如果採用4位元來檢測，則有用的資料長度可達 11 位元」了。

賴昭正：美國芝加哥大學化學博士