What's fun in EE

臺大電機系科普系列

為何傳簡訊、email 很少出錯？漫談通訊與通道編碼技術

葉丙成／臺大電機系教授

隨著通訊科技的進步，我們只要彈指之間便可以將簡訊或是 email 傳遞到千里之外。其實在數千年前地球上就有高速廣域光通訊系統的存在了。別以為我是衛斯理的故事看太多了？（說來確實還看過不少！）我要提的是太史公在史記周本紀裡所寫的，二千七百年前周幽王烽火戲諸侯以博褒姒一笑的故事，這也是大家所熟知的中國版狼來了。太史公所提到的烽火，是古人用來傳遞敵軍來犯戰報的方法。從邊疆一直到國都，每隔固定的距離便設置一座烽火台。一旦有敵人來犯，烽火台便會點燃烽火，一站一站的接力傳遞訊息到國都，傳遞的速度相當的快。相傳漢朝霍去病在河西（甘肅附近）跟匈奴打仗時，戰報不用一晝夜便可透過烽火傳遞到數千里外的遼東（朝鮮半島）。在千年前能利用光（烽火）將訊息傳遞速度如此之快、距離如此之遠，這可不是一種令人讚嘆的高速廣域光通訊系統？這種通訊方式維持了兩千多年，一直到了明清時期都還在使用。

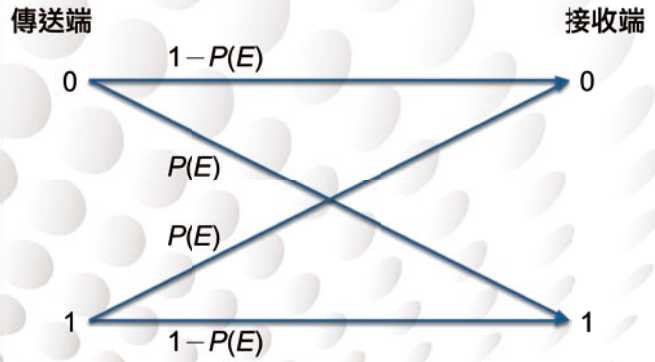
圖一　西安驪山烽火台，相傳為周幽王烽火戲諸侯之遺址。台前碑文：周烽火台故址
（http://www.guanjiayou.com/sights/view/13653.htm）

臺灣大學電機工程學系
10617 台北市 大安區 羅斯福路四段 一號
Email: dept@cc.ee.ntu.edu.tw
http://www.ee.ntu.edu.tw/

雖然古人這種廣域光通訊系統相當酷，不過它還是有很大的限制。第一，它能傳的訊息量很少。墨子雜守篇裡提到「… 望見寇，舉一峰；入境，舉二峰；射妻，舉三峰；郭會，舉四峰二藍；城會，舉五峰五藍 …」，也就是說透過烽火只能傳遞五種不同的戰況。以今日常用來計算資訊量的位元（bit）來說，用三個位元可以表示二的三次方也就是八種不同的資訊。而烽火只能傳遞五種戰況，其資訊量還不到三位元，實在很少。烽火的第二個限制是環境的干擾。因為烽火是靠火和視覺在傳遞的，所以最忌諱的是大雨跟大霧對點火和視覺的干擾。這些環境的干擾可能導致對戰況的判讀錯誤，造成嚴重後果。因此後來烽火制度經過改良，搭配擊鼓次數來傳遞訊息。如此說來古人老早就有了同時利用光跟聲音的廣域多頻通訊技術，真是有意思極了（請原諒電機工程師的自我陶醉）。

就如同烽火傳遞會受到環境因素的干擾而可能出錯，現代的通訊也有同樣的問題。我們常常有這樣的經驗，在電梯或地下室裡用手機講電話的時候，聲音常常很不清楚或是斷線。不過傳簡訊或是送電子郵件時，倒是很少出現訊息錯誤。電機工程師們到底是什麼樣的方法讓我們傳遞訊息時幾乎都不會出錯呢？這個問題我們平常很少去注意它。電機工程師們所開發出來的通訊技術總是默默的幫我們傳遞正確無誤的訊息，讓我們以為這麼可靠的服務是理所當然的，就好像我們常常忽略了老媽對我們的默默付出一樣。其實這裡面可是大有學問的哩！為了提高訊息傳遞的正確性，電機工程師開發了許多技術。其中最重要的便是所謂的通道編碼技術（channel coding）。 如果沒有通道編碼技術的存在，整個世界可能會天下大亂。這可不是我危言聳聽。大家想像一下，如果沒有通道編碼技術而使得資訊傳遞常常發生錯誤：當有人轉帳一千塊結果銀行收到的訊息是要匯出一百萬；當有人買機票要去馬德里結果航空公司把他送去新德里；當有人在線上遊戲裡要把某個寶物給朋友結果系統收到訊息是他要把所有的家當都送出去。這些事情想想都讓人覺得可怕！仔細想想，正確可靠的通訊是我們現代文明的重要基石之一。一旦失去了通訊的正確性，人類的文明生活很有可能完全崩潰。究竟通道編碼技術是如何幫助我們提高通訊的正確性和可靠度的呢？

要介紹通道編碼技術之前，我們得先了解一下資訊是怎麼傳遞的。通常我們所要傳遞的資訊，不管是聲音、文字、圖畫等，都會先被轉化成一堆 0 或 1，也就是所謂的資料位元。轉化成位元之後，再從傳送端以電波的形式傳遞出去，由接收端接收。傳遞的過程中，這電波除了受到外界電磁波的干擾外，也會受到通訊裝置內部電路本身的雜訊所影響。其中電路雜訊的來源主要是因為熱能的關係。只要溫度不是絕對零度，就會有電子因為熱能的關係變得很 high。我們都知道人一 high，行為就很難受控制。電子也是一樣，一 high 起來後，明明電位差是讓它該往某個方向走，偏偏它卻亂衝亂跑不受控制。因此電路上的電流會跟我們預期的值不一樣，其中的差異就是所謂的雜訊。由於外界電磁波的干擾和內部電路的雜訊影響，位元在透過電波的傳遞時，是有相當的可能會出錯的。當我們用高能量傳送電波時，電波相對於干擾和雜訊而言很強，位元出錯的機率會變小；相反的能量低的時候出錯的機率會變高。因此嚴格說來，這個位元出錯機率是每單一位元所耗費的能量 E 的函數，我們以 $p(E)$ 來表示它。這樣的通訊模型，如圖二所示。特別注意的是，從圖二我們可以看見兩種位元出錯的情況。不管是傳 0 錯成 1 或是傳 1 錯成 0，發生機率一樣是 $p(E)$；而無論是傳 0 或是 1，被正確收到的機率都是 $1 - p(E)$。



圖二　簡單的位元通訊模型（Binary symmetric channel model）

有了這個模型，我們就可以計算一下通訊發生錯誤的機率。舉例來說，假設我們現在想傳遞三個位元的資料。這三個位元可能是 000、001、010、011、100、101、110、111 這八種組合中的任何一種。假設我們傳 000，而接收端要真能成功收到 000，前提便是三個位元在傳送過程中都沒有出錯。因此三個位元被成功接收的機率是

$$(1 - p(E)) \times (1 - p(E)) \times (1 - p(E)) = 1 - 3p(E) + 3(p(E))^2 - (p(E))^3 \quad (1)$$

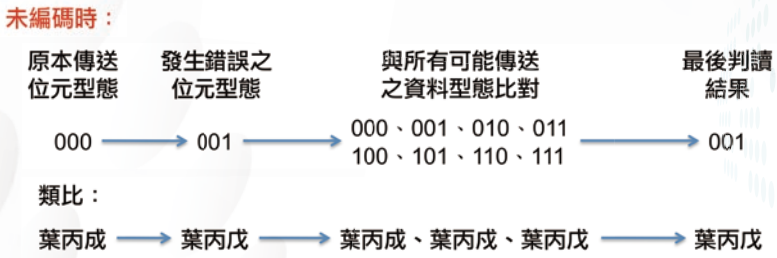
相對的，傳遞過程會出錯的機率是 1 減掉成功的機率，亦即

$$P_u(E) = 1 - [1 - 3p(E) + 3(p(E))^2 - (p(E))^3] = 3p(E) - 3(p(E))^2 + (p(E))^3 \quad (2)$$

今天如果我們每個位元所使用的能量 E 剛好使得每個位元出錯的機率 $p(E) = 0.00001$ 時，則 $P_u(E) \fallingdotseq 0.00003$。也就是說，當我們傳遞資料時，有將近三萬分之一的比例會出錯。

那有沒有方法可以減少錯誤的發生呢？有的，這就是要靠電機工程的通道編碼技術。在談通道編碼的原理前，我先講一個故事。從前有三個兄弟，分別叫做葉丙成、葉丙戍、葉丙戊。其中葉丙成跟葉丙戍兩個在念小學的時候很不用功，數學常常考零分。更糟糕的是他們連名字也不大會寫，一個常常會忘了寫「成」裡面那一筆劃的耳朵，另一個常常忘了「戍」裡面那一點。老爸每次看到考卷都以為是葉丙戊考零分，可憐的葉丙戊常常就被莫名其妙的修理一頓。

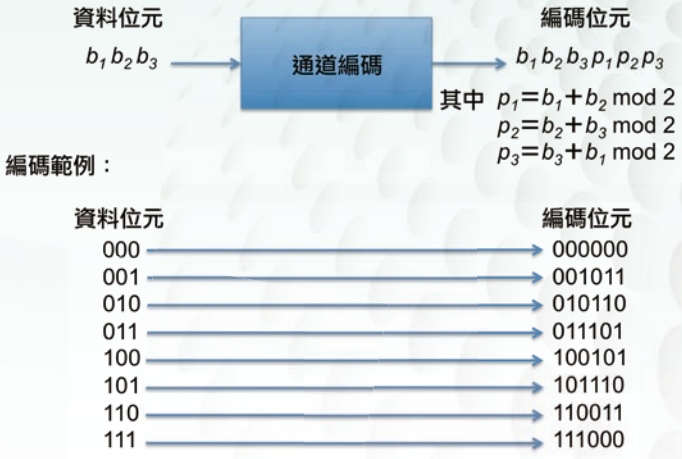
為什麼老爸會有這種錯誤呢？原因是三兄弟的名字太像了，只有一個筆劃不同。當那兩個渾小子少寫一筆劃的時候，老爸根本無從判斷這個考卷是真的葉丙戊的，還是葉丙成或葉丙戍寫錯名字。老爸只能假設這真的是葉丙戊的考卷。之前傳三個位元也是類似的情形。就如同圖三中的範例，當人家傳 000 時如果傳遞過程中有一個位元出錯了，使得我們接收到 001。因為 001 本身也是有可能被傳出來的八種資料型態之一，當我們看到 001 時，我們就像老爸一樣無從判斷是人家是本來就傳 001 給我們，抑或是人家傳 000 錯成 001。因為通常位元出錯的機率 $p(E)$ 不是很大，所以我們常會採信人家本來就是傳 001 給我們，解讀錯誤也就這麼發生了。



圖三　未使用通道編碼時易造成判讀錯誤

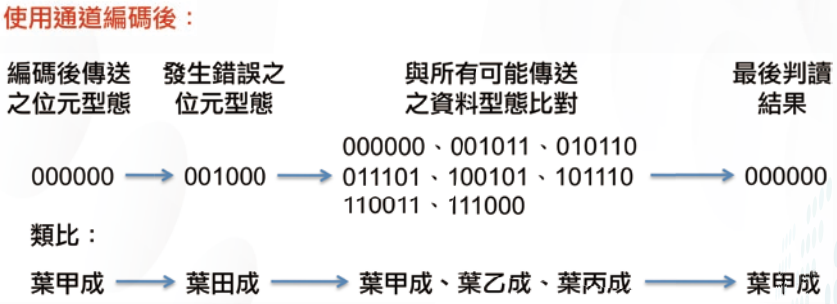
那要怎麼解決這問題呢？我們再回到三兄弟的故事。如果他們的老爸夠聰明的話，應該把三兄弟帶去戶政事務所改名字，改成葉甲成、葉乙成、葉丙成。這時候即使葉甲成有個筆劃寫錯，老爸看到零分考卷上的名字「葉田成」，馬上發出會心的一笑，直接修理葉甲成。為什麼呢？這是因為三個名字的差異夠大。即使寫錯了一兩個筆劃，老爸還是很容易看出這個寫錯的名字跟誰的最像，進而還原正確的名字。這正是通道編碼的原理：讓傳遞的資料型態差異夠大，即使傳遞過程有位元出錯，我們還是有機會解讀出正確的內容。

我們先以圖四中的簡單通道編碼做範例。當要傳資料位元 $b_1\ b_2\ b_3$ 時，我們經由通道編碼加入了三個檢查位元 $p_1\ p_2\ p_3$ ，因此編碼後變成六個位元 $b_1\ b_2\ b_3\ p_1\ p_2\ p_3$。其中我們讓 p_1 等於 $b_1 + b_2$ 除以 2 的餘數，數學上表示成 $p_1 = b_1 + b_2 \bmod 2$。也就是說 p_1 中隱含著關於 $b_1 + b_2$ 奇偶性的資訊：當 $b_1 + b_2$ 為奇數時 $p_1 = 1$；$b_1 + b_2$ 為偶數時則 $p_1 = 0$。同理 p_2 和 p_3 分別隱含著 $b_2 + b_3$ 與 $b_3 + b_1$ 奇偶性的資訊。在編碼以前，我們發現 000 跟 001 這兩種資料型態只有一個位元不同。可是在編碼後，他們分別變成 000000 跟 001011，差別變大了！這有什麼好處呢？



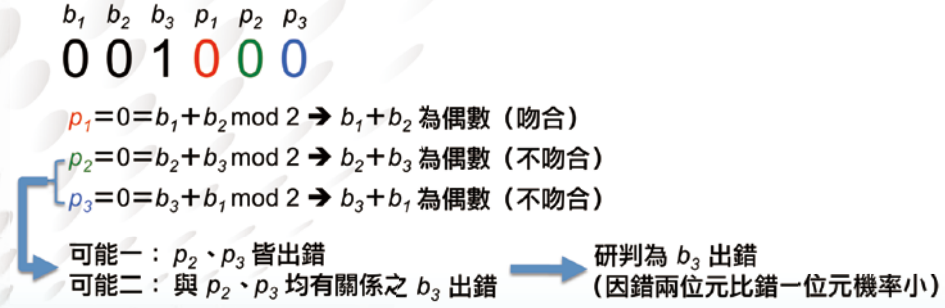
圖四　簡單的通道編碼範例

我們考慮圖五中的例子：假設人家編碼後傳 000000 給我們的時候有一個位元出錯，使得我們收到 001000。我們把 001000 跟八種可能的編碼位元型態做比對，發現它跟 000000 只有一個位元的差別，跟其他七種編碼位元型態都至少有兩個以上的位元不一樣。就如同老爸可以很快的把「葉田成」判讀成「葉甲成」一樣，我們也是很快的就可判讀出人家最有可能傳給我們的是 000000，也就是資料位元是 000。能做這個結論最主要是因為傳遞過程會那麼倒楣有兩個以上位元出錯的機會，比只錯一個位元的機會小很多。



圖五　使用通道編碼後可減少判讀錯誤的發生

透過圖五的例子，我們發現通道編碼之所以有用，是因為它能讓不同的資料位元型態在編碼後差異變得更大。差異變大，使得我們對於錯誤發生的容許度變高，錯了一個位元的話我們也能更正回來。除了這個觀點外，我們還可以從另一個好像偵探辦案的有趣角度來看通道編碼。前面說到，p_1、p_2、p_3 分別代表了 $b_1 + b_2$、$b_2 + b_3$、$b_3 + b_1$ 的奇偶。當我們如圖六所示收到 001000 時，李組長眉頭一皺，直覺案情並不單純。根據收到的結果，$b_1\ b_2\ b_3$ 似乎是 001。可是根據證人 $p_2 = 0$ 的供詞，$b_2 + b_3$ 是偶數。另外證人 $p_3 = 0$ 也提到了 $b_3 + b_1$ 是偶數。這兩個人的證詞跟我們看到 $b_1\ b_2\ b_3$ 是 001 的觀察是不吻合的。究竟是 $b_1\ b_2\ b_3$ 三人中有人出事被假冒了，還是 p_2 和 p_3 這兩個證人有問題？案情似乎曲折離奇、匪夷所思。不過英明的李組長發現，在所有可能的情形當中，如果 p_2 和 p_3 中有任何一個人說謊，則 $p_1 = 0$ 的證詞絕對是偽證（Why? 試著證看看！）。如此便會出現兩個證人都做偽證，這發生的機率實在很低。因此李組長先假設證人都沒做偽證。在這種情形下，由於只有 p_2 和 p_3 的證詞跟我們看到 $b_1\ b_2\ b_3$ 是 001 的觀察是不吻合的，而這兩個證人都跟 b_3 有關係！英明的李組長馬上發現 $b_3 = 1$ 是假貨的機率很高，進而斷定 $b_1\ b_2\ b_3$ 應該是 000 才對！



圖六　利用檢查位元研判錯誤位元所在位置

各位有沒有覺得通道編碼的解碼過程好像偵探在辦案一樣有趣呢？從這另一個角度來看，通道編碼所做的就是把跟資料位元有關的資訊藏在 p_1、p_2、p_3 之中。這些位元我們通常稱為檢查位元。當人家要傳資料給我們時，會把資料位元跟檢查位元一起傳過來。傳遞過程中如果有錯誤發生，我們便可以像李組長一樣從檢查位元中的蛛絲馬跡來查出到底最有可能出錯的是哪個位元。不過我們解碼的過程不用像李組長辛苦的推敲老半天。透過數學跟通道編碼理論的推導，我們能用很有效率的數學方法來完成解碼的過程，這也使得通道編碼技術得以廣泛的被利用。

話說回來，我們如何確定通道編碼真的有降低判讀錯誤的機率呢？我們可以簡單的算算看。假設今天人家要傳給我們的資料位元是 000。經過編碼後傳出來的是 000000。我們把 000000 跟其他七個編碼結果比較，發現有四個編碼結果跟 000000 有三個位元不同；有三個編碼結果跟 000000 有四位元不同。因此在傳遞過程中如果有一個位元出錯，不管是在哪個位置發生，000000 都會比其他七個編碼結果更接近我們所接受到的六個位元（只有一個位元不同）。也就是說只有一個位元出錯的話，我們一定不會判讀錯誤。因此說起來，我們判讀成功的機率至少有

$$(1-p(E))^6 + C_{6,1}(1-p(E))^5 p(E) = (1-p(E))^6 + 6(1-p(E))^5 p(E) \tag{3}$$

也就是會出現判讀錯誤的機率 $P_c(E)$ 不會超過

$$P_c(E) < 1 - [(1-p(E))^6 + 6(1-p(E))^5 p(E)] \tag{4}$$

如果我們直接把第 (4) 式中的上界直接去跟沒做編碼時的第 (2) 式做比較，是不公平的，原因是我們編碼後傳六個位元時，每個位元所傳的能量都還是 E。也就是說，我們花了 $6E$ 的能量來傳編碼後的位元。可是原先沒做編碼的情況下，我們只傳三個位元，總共花了 $3E$ 的能量。各位想想看，這樣子比較，公平嗎？這就好比在一個廚藝大賽中，有一個阿鴻師拿了六千塊的材料費買食材，而另一個阿丙師只分到三千塊買便宜的食材。比賽結果就算阿鴻師贏了，心胸狹窄的阿丙師也絕對不會覺得是自己的廚藝不如人。為了要有公平的比賽，我們應該要給他們一樣多的預算去買食材。這樣阿丙師輸的時候才會雞嘴變鴨嘴，知道自己是真的廚藝不如人。同樣的道理，我們不管有用編碼或是沒用編碼，花在傳遞位元的總能量應該要一樣。如果第 (2) 式中沒用編碼時，每個位元都花費能量 E 傳遞，那表示總能量是 $3E$。因此當有編碼的時候，每個編碼後位元應該只能花費 $3E/6 = 0.5E$ 的能量傳遞。所以我們要比較的應該是第 (2) 式的 $P_u(E)$ 與第 (4) 式中 $P_c(0.5E)$ 的上界

$$P_c(0.5E) < 1 - [(1-p(0.5E))^6 + 6(1-p(0.5E))^5 p(0.5E)] \tag{5}$$

在 $p(E) = 0.00001$ 時我們算過第 (2) 式 $P_u(E) \fallingdotseq 0.00003$；而此時 $p(0.5E)$ 從其他通訊理論可算出約為 0.001，帶入第 (5) 式得到 $P_c(0.5E) < 1 - [(1-0.001)^6 + 6(1-0.001)^5(0.001)] = 0.000015$。我們可以看到判讀錯誤的機率大幅降低到原來的二分之一！而且不要忘記我們用的只是一個非常簡單的通道編碼。事實上在手機及各式各樣的通訊裝置上所用的通道編碼，結構遠比我們這裡所用的複雜，更正錯誤的能力也因而更加優越。這也是為什麼我們平常通訊出錯的機會很小，一切都有賴於通道編碼技術對資料的保護。

在現今的世界，通訊無所不在。人們在無時無刻都在通訊：用電腦、聽數位廣播、看數位電視、講電話、發簡訊、…，裡面在在用到通道編碼。除了通訊之外，像是硬碟資料、CD 唱片、DVD 等儲存技術也都用到通道編碼來提高資料儲存的可靠度。此外，甚至連我們的身分證字號也有用到通道編碼喔！大家有沒有發現有時候在某些系統輸入身分證字號，如果我們隨意給一個號碼都不會過關？這就是因為身分證字號中也暗藏有檢查碼的存在，所以系統才能檢測出我們輸入的身分證字號不正確。同樣的方法也應用在各式證件的號碼中。如果沒有通道編碼技術存在，我們的世界真的會因此而大亂！所以前面說到它是現代文明的重要基石之一，一點也不為過。通道編碼方面的研究主要都是由電機學者還有數學家們所推導出來的，其中最有名的大師是身兼電機工程師與數學家身分的夏農（Claude Shannon, 1916-2001）。夏農所推導出的一連串精采而漂亮的數學理論，成為我們今日通道編碼以及數位通訊技術的重要基石。下次當你我在享受現代通訊科技所帶來的便利生活時，千萬不要忘記夏農和其他電機、數學家的功勞喔！