**期末project、BCH Code**

1. **原理介紹**

BCH碼為取自Bose、Ray-Chaudhuri與Hocquenghem的縮寫，是用於校正多個隨機錯誤模式的多級、循環、錯誤校正、變長數字編碼，BCH碼也可以用於質數級或者質數的冪級的多級相移鍵控。

BCH 碼使用有限域上的域論與多項式，要構建一個能夠檢測、校正兩個錯誤的BCH碼，我們要使用有限域GF(16)。如果α是m1(x) = x4 + x + 1的一個根，那麼m1就是α的極小多項式，這是因為

m1(x) = (x -α)(x -α2)(x -α4)(x - α8)=x4 + x + 1。

如果要構建一個能夠糾正一個錯誤的 BCH 碼，那麼就使用 m1(x)，這個代碼就是所有滿足C(x)≡0（mod m1(x)）且根為α、α2、α4、α8 的多項式 C(x)。

編碼

構建碼字為 (c14, c13, ..., c8)，這樣多項式為c14+c13+...+c8，我們將它稱為 CI。接著就要找出CR滿足CR=CI (mod m1,3(x))=c7+c6+...+c0，這樣就得到待發的碼字C(x) = CI+CR (mod m1,3(x)) = 0

例如：我們對(1,1,0,0,1,1,0)進行編碼CI=x14+x13+x10+x9，然後用 m1,3(x) 除以CI，得到結果為CR(x)=x3+1，這樣待發的碼字為(1,1,0,0,1,1,0, 0,0,0,0,1,0,0,1)

解碼

BCH 的解碼過程可以分為以下四個步驟：

1. 計算接收到的向量 R 的 2t 伴隨矩陣

2. 計算錯誤定位多項式

3. 解多項式，得到錯誤位置

4. 如果不是二進位 BCH 碼，就計算錯誤位置的誤差值

假設我們收到一個碼字向量 r，即多項式 R(x)），如果沒有錯誤，那麼 R(α)=R(α3)=0；如果有一個錯誤，例如r = c + ei，其中ei表示R14的第 i個基向量，於是S1 = R(α) = C(α) + αi = αi，S3 = R(α3) = C(α3) + (α3)i = (αi)3 = S13，這樣就可以糾正錯誤。α的指數顯示的數據位變化可以幫助我們校正錯誤；如果有兩個錯誤，r = c + ei + ei，那麼S1=R(α)=C(α)+αi+αj，S3=R(α3)=C(α3)+ (α3)i + (α3)j = (α3)i + (α3)j，這與S13不同，所以我們認為有兩個錯誤。

1. **程式碼**

這次的作業我使用的軟體是MATLAB，程式碼如圖2所示：

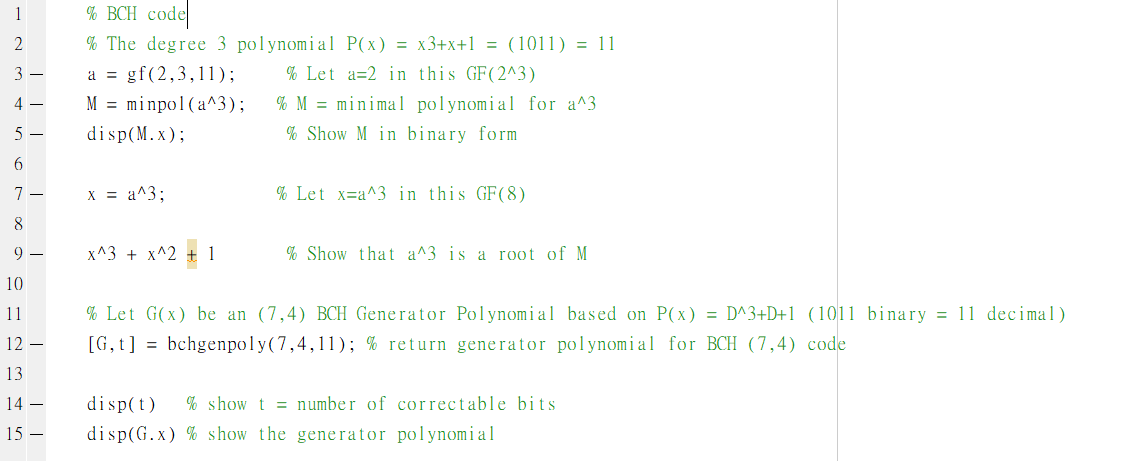


圖2

1. **執行結果**

如圖3所示：

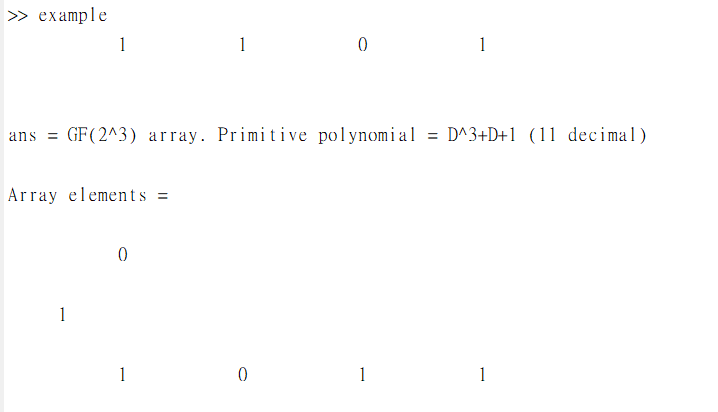


圖3