崑山科技大學學報第四期 第 23~32 頁（民國 96 年 7 月）
Journal of Kun Shan University, Vol.4, pp.23~32（Jul, 2007）

二次剩餘碼在連接結構上的特性探討

葉蘭英

崑山科技大學電子工程系 助理教授

摘要

在本文章中，我們應用二次剩餘碼(Quadratic Residue Codes)到結構(u，v)與結構(u，u+v) 以建立新的連接電碼(Concatenated Codes)。首先介紹符號、定義與二次剩餘碼的特性探討，其次介紹結構(u，v)與結構(u，u+v)的特性。最後提出這些連接電碼編解碼的方法。

關鍵詞：二次剩餘碼、連接結構、連接電碼、分圓陪集

壹、符號與定義

本段落先介紹一些本篇文章需要用到的符號與定義。為了簡化與易懂，在本文中除非特別註明，否則我們所考慮的電碼 (code) 都是二元線性的 (binary and linear)。 [n,k] 電碼(code) C 是一個 n 維空間的 k 維子空間。 [n,k,d] 電碼表 [n,k] 電碼，有最小加權值 d，即所有碼字元的加權值都大於等於 d。若兩個電碼 C_1，C_2 之間唯一不同的地方僅止於元素註標的重新排列而已，則稱這兩個電碼等價(equivalent)，表示為 $C_1 \sim C_2$。任意給定 n 與 k，一般我們希望 d 越大越好，如此可增加該電碼訂正錯誤的能力。

GF(q)表有限體(finite field)。若 $v=(v_0,v_1,...,v_{n-1})$與 $u=(u_0,u_1,...,u_{n-1})$是佈於 GF(q)上的向量,則 $v \cdot u=\sum_{i=0}^{n-1} v_i u_i$ 。若 C 是一個[n,k]碼,則它的對偶碼 $C^{\perp}$ (dual code)定義為 $C^{\perp}=\{u|v \cdot u=0(\text{mod } q), v \in C\}$， 是一個[n,n-k]電碼。若 $C \subset C^{\perp}$則稱 C 是自正交碼(self-orthogonal code)。若 $C = C^{\perp}$則稱 C 是自對偶碼(self-dual code)， 此時 n 必為偶數且 k=n/2 (因 n-k=k)。$\underline{C}$ 表 C 的擴充碼 (extended code)，定義為 $\underline{C}=\{(v_0, v_1 ,...,v_n)| \sum_{i=0}^{n} v_i =0(\text{mod } q), (v_0,v_1,...,v_{n-1}) \in C\}$。向量 $v= (v_0,v_1,...,v_{n-1})$， 若 $\sum_{i=0}^{n-1} v_i =0(\text{mod } q)$，則稱 v 是似偶向量(even-like vector)。否則稱 v 為似奇向量(odd-like vector)。若電碼 C 的所有元素都是似偶(奇)向量，則稱 C 為似偶(奇)電碼。

貳、 二次剩餘碼的特性探討

G 表在 GF(p)上非零元素組成的乘法群(multiplicative group)。令 $Q=\{r^2 \pmod p | r\in G\}$ 表 G 中的所有二次剩餘(quadratic residue)且 N=G-Q 表 G 中非二次剩餘(nonresidue)。在討論二元 QR 碼時，我們假設質數 $p\equiv\pm1 \pmod 8$，以確保 $2\in Q$。考慮一個數 s $(0\leqq s\leqq p-1)$，若 m 為滿足 $2^m s \equiv s \pmod p$的最小整數，則可定義一個包含 s 的分圓陪集(cyclotomic coset)c_s 為 $\{s,2s,2^2s,...,2^{m-1}s \pmod p\}$。每個分圓陪集有 m 個元素且因此有 k 個分圓陪集，其中 mk=p-1。依陪集的特性， 二次剩餘 Q 與非二次剩餘 N 皆由 k/2 個分圓陪集構成。令 $e_1(x)=\sum_{i\in Q} x^i$ ，$e_2(x)=\sum_{i\in N} x^i$ 佈於 GF(2)。 $e_i^2(x)=e_i(x)$ 。因此 $e_1(x)$，$e_2(x)$都是等冪式 (idempotent)。

定義：質數 $p\equiv\pm1 \pmod 8$。長度為 p 的二元循環碼，若它的等冪生成式是 $e_1(x)$，$e_2(x)$，$1+e_1(x)$或 $1+e_2(x)$則稱此循環碼為二元二次剩餘碼(binary QR code)。

因此對於任何一個質數 $p\equiv\pm1 \pmod 8$，依上面的定義，有兩對(四個)長度 p 的二元 QR 碼。對於一般非二元的二次剩餘碼 e(x)不容易找到，所以我們是這樣定義的：

定義：l 是 mod p 的二次剩餘，α是在 GF(l)的擴充體中，單位元的 p 次原始方根 (primitive p-th root of unity)。$q(x)=\prod_{i\in Q}(x-\alpha^i)$ ，$n(x)=\prod_{i\in N}(x-\alpha^i)$，$q(x)，n(x)\in GF(l)[x]$。佈於 GF($l$)長度為 p 的循環碼 C，若它的生成多項式是 $q(x)，n(x)，(x-1)q(x)$或 $(x-1)n(x)$，則稱 C 為二次剩餘碼 (QR code)。

以上兩種 QR 碼的定義，在二元的情況下是等價的。非二元的 QR 碼，e(x)的建立請見[1, p485]。

對於存在 QR 碼的任意長度 p，有兩對電碼$(Q_1,Q_2)(Q'_1, Q'_2)$，其中 $Q_1 \sim Q_2$，$Q'_1 \sim Q'_2$，且分別是$[p,(p+1)/2, d\geqq \sqrt{p}\,]$，$[p,(p-1)/2,d\geqq \sqrt{p}\,]$循環碼。QR 碼的特點是 k/p 比值接近 1/2 且比值 $d/p\geqq 1/\sqrt{p}>>0$。它的解碼方法很多[1, p512]， 最常用的是排列解碼法 (permutation decoding)。

定理 1：質數 $p\neq2$，在有限體 GF(p)中有一半非零元素是 mod p 的二次剩餘 Q 與另一半是非二次剩餘 N，即 $Q\cup N\cup\{0\}=\{0,1,2,..,p-1\}$且$|Q|=|N|=(p-1)/2$。

證明：$\forall a\in GF(p)-\{0\}$，$a^2=(-a)^2=(p-a)^2 \pmod p$， 因此 $Q=\{1^2,2^2,..,((p-1)/2)^2 \pmod p\}$。Q 中任意兩元素 i，j， $1\leq i，j\leq(p-1)/2$。若 $i^2=j^2 \pmod p$則 $(i+j)(i-j)=0 \pmod p$。因 p 是質數，所以 $p|(i+j)$ 或 $p|(i-j)$，但 $2\leq i+j\leq p-1$， $(p-3)/2\leq i-j\leq(p-3)/2 \Rightarrow i-j=0$，即 i=j。所以

Q 中每個元素都相異⇒ |Q|=(p-1)/2。N={1,2,..,p-1}-Q⇒ |N|=(p-1)/2。 Q.E.D.

例 1：設 p=31，mod 31 的二次剩餘 $Q=\{1^2,2^2,3^2,4^2,..,15^2 \pmod{31}\}$ = {1,2,4,5,7,8,9,10,14,16, 18,19, 20,25,28}，|Q|=15=(31-1)/2。
N={3,6,11,12,13,15,17,21,22,23,24,26,27,29,30}，|N|=15。
$\mu_{-1}(Q)$={-1,-2,-4,-5,-7, -8,…,-28}={30,29,27,26,24,23,..,3}=N。

由例 1，$\mu_{-1}(Q)=N$。其實對於任何一個 a∈ N，q∈ Q，$\mu_a(q)=aq$，可得 $\mu_a(q) \in N$，因此我們定義的μ_a :Q→N 有以下特性：

推論 1：任意質數 p 與 a∈ N，
(i) μ_a :Q→N 是一對一映成函數(one-to-one onto mapping)。
(ii)若 p≡ -1 (mod 8)，則μ_{-1}:Q→N 也是一對一映成函數。

定理 2：若循環碼 C 有等冪生成式 e(x)，則 $C^{\perp}$有等冪生成式 $1-\mu_{-1}(e(x))$。
證明：令 $e(x)=a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{n-1}$，$1-e(x)=(1-a_0)-a_1x-a_2x^2-\ldots-a_{n-1}x^{n-1}$。
$e(x)(1-e(x))=e(x)-e^2(x)=0$，由 [2, p66]
⇒ $(a_0,a_1,\ldots,a_{n-1})$ 與 $(-a_{n-1},-a_{n-2}..,-a_1,1-a_0)$的所有循環位移正交(orthogonal)。
$\mu_{-1}(1-e(x))=(1-a_0,-a_{n-1},-a_{n-2},..,-a_1)=1-(a_0,a_{n-1},a_{n-2},..,a_1)=1-\mu_{-1}(e(x))$。 e(x)與$\mu_{-1}(1-e(x))$的所有循環位移正交。$(1-e(x))^2=1-2e(x)+e^2(x)=1-e(x)$
⇒ 1-e(x)也是等冪式。由 [1, 引理 4, p219] $\mu_{-1}(1-e(x))$也是等冪式⇒ $C^{\perp}$有等冪生成式 $\mu_{-1}(1-e(x))=1-\mu_{-1}(e(x))$。 Q.E.D.

引理 1：質數 p≡ -1 (mod 8)，令 $q(x)=\prod_{i\in Q}(x-\alpha^i)$，$n(x)=\prod_{i\in N}(x-\alpha^i)$，α是單位元素的 p 次原始方根 (primitive p-th root of unity)， 則
(i) q(x)的反商多項式(reciprocal) q*(x)為 n(x)的常數倍。
(ii) n(x)的反商多項式 n*(x)為 q(x)的常數倍。
證明：(i) $x^p-1=(x-1)q(x)n(x)$，q(x)有根集合$\{\alpha^r : r\in Q\}$，n(x)有根集合$\{\alpha^r : r\in N\}$。由定理 1 與反商多項式的定義，$q^*(x)=x^{\{p-1\}/2}\prod_{i\in Q}(x^{-1}-\alpha^i)=\prod_{i\in Q}(\alpha^{-i}-x)\alpha^i$ ，由推論 1 (ii)， -1∈N
⇒ q*(x)有根集合是。$\{\alpha^{-r} : r\in Q\}=\{\alpha^r : r\in N\}$。但 deg(n(x))={p-1}/2 且 deg(q*(x))= deg(q(x))={p-1}/2 ⇒ q*(x)為 n(x)的常數倍。同理可證(ii)。 Q.E.D.

定理 3： p≡ -1 (mod 8)，Q，N，q(x)，n(x)，α的定義如引理 1。若 Q_1，Q_2，Q'_1，Q'_2 是分別以 q(x)，n(x)，(x-1)q(x)，(x-1)n(x)為生成多項式的 QR 碼，則
(i)dim Q_1=dim Q_2=(p+1)/2，dim Q'_1= dim Q'_2=(p-1)/2。
(ii) Q_1= Q'_1+< h(x)>， Q_2= Q'_2+< h(x)>，$Q_1\cap Q_2$=< h(x)>，且

$Q_1+ Q_2= Rp = GF(l)[x]/< x^p-1>$。

(iii) $Q'_1 \cap Q'_2=\{0\}$，$Q'_1+ Q'_2=\{$Rp 中所有似偶向量$\}$。

(iv) $Q_1 \sim Q_2$，$Q'_1 \sim Q'_2$。

(v) Q'_1， Q'_2 都是自正交碼 (self-orthogonal code) 且 $Q^{\perp}_1= Q'_1$，$Q^{\perp}_2= Q'_2$。

(vi)$d^2-d+1 \geq p$，其中 d 是 Q_1，Q_2 的最小加權值(minimum weight)。

證明：(i) 由定理 1，$|Q|=|N|=(p-1)/2= \deg(q(x))= \deg(n(x))$

$\Rightarrow \dim Q_1=\dim Q_2=(p+1)/2$。$\deg((x-1)q(x))= \deg((x-1)n(x))=(p-1)/2+1=(p+1)/2$

$\Rightarrow \dim Q'_1= \dim Q'_2 = p-(p+1)/2 = (p-1)/2$。

(ii) $Q_1 \cap Q_2$ 的生成多項式是 $\text{lcm}(n(x),q(x))= \text{lcm}(\prod_{r\in Q}(x-\alpha^r), \prod_{r\in N}(x-\alpha^r))$

$=(1+x+x^2+\ldots+x^{p-1})$

$\Rightarrow Q_1 \cap Q_2=< h(x)>$。$\dim(Q_1+Q_2)= \dim(Q_1)+ \dim(Q_2)- \dim(Q_1 \cap Q_2)=(p+1)/2+(p+1)/2-1=p$

$\Rightarrow (Q_1+Q_2)=Rp=GF(l)[x]/ < x^p-1>$。 由 Q_1，Q_2，Q'_1，Q'_2 的生成多項式

$\Rightarrow Q'_1 \subset Q_1$，$Q'_2 \subset Q_2$，且因 Q'_1，Q'_2 的生成多項式有因子$(x-1)$，所以 Q'_1，Q'_2 的元素都是似偶向量(even-like vector)

$\Rightarrow Q'_1 \cap < h(x)>=\phi$， $Q'_2 \cap < h(x)>= \phi$。因 $\dim Q_1= \dim Q'_1+1$， $\dim Q_2= \dim Q'_2+1$，且 $h(x) \in Q_1 \cap Q_2$，所以 $Q_1= Q'_1+< h(x)>$，$Q_2= Q'_2+< h(x)>$。

(iii) $Q'_1 \cap Q'_2$ 的生成多項式是 $\text{lcm}((x-1)q(x),(x-1)n(x))=(x-1)q(x)n(x)=x^p-1=0$

$\Rightarrow Q'_1 \cap Q'_2 =\{0\}$。 $Q'_1 \cup Q'_2$ 的生成多項式是$((x-1)q(x),(x-1)n(x))=(x-1)$

$\Rightarrow Q'_1 \cup Q'_2 =\{$Rp 中所有似偶元素$\}$。

(iv)由推論 1，$\forall a \in N, \mu_a : Q \rightarrow N$ 是一對一映成。同理$\mu_a: Q_1 \rightarrow Q_2$，$\mu_a : Q'_1 \rightarrow Q'_2$ 也是一對一映成。因此 $Q_1 \sim Q_2$，$Q'_1 \sim Q'_2$。

(v) $Q'_1 =<(x-1) q(x)>$，$Q'_2=<(x-1)n(x)>$且 $x^p-1=(x-1)q(x)n(x) \Rightarrow (Q'_1)^{\perp}$，$(Q'_2)^{\perp}$分別有生成多項式 $n^*(x)$，$q^*(x)$。由引理 1，$n^*(x)$，$q^*(x)$分別是 $q(x)$,$n(x)$的常數倍

$\Rightarrow n^*(x) | (x-1)q(x)$，$q^*(x) | (x-1)n(x)$

$\Rightarrow Q'_1 \subset (Q'_1)^{\perp}$， $Q'_2 \subset (Q'_2)^{\perp}$

$\Rightarrow Q'_1$， Q'_2 都是自正交碼。Q_1 有生成多項式 $q(x) \Rightarrow Q_1^{\perp}$有生成多項式 $((x-1)n(x))^*=(1-x)n^*(x)$。由引理 1，$Q_1^{\perp} =<(1-x)n^*(x)>=<(x-1)q(x)>= Q'_1$，同理 $Q^{\perp}_2= Q'_2$。

(vi)見[2, p90]。

推論 2：[1, 定理 2, p484]若 $l=2$，且 N，Q，q(x)，n(x)的定義同前，則α可以適當的選擇使得 Q_1，Q_2，Q'_1，Q'_2 分別有等冪生成式 $e_1(x)=\sum_{i\in Q} x^i$，$e_2(x)= \sum_{i\in N} x^i$，$1+ e_1(x)$，$1+ e_2(x)$。

例 2：p=31，由例 1，Q={1,2,4,5,7,8,9,10,14,16,18,19,20,25,28}，N={3,6,11,12,13,15,17, 21,22,23, 24,26,27,29,30}，有 4 個二元 QR 碼 Q_1，Q_2，Q'_1，Q'_2 分別如下：

	Q_1	Q_2	Q'_1	Q'_2
生成多項式	$1+x+x^2+x^6$ $+x^7+x^{12}+x^{15}$	$1+x^3+x^8+x^9$ $+x^{15}+x^{14}+x^{15}$	$1+x^3+x^6+x^8$ $+x^{12}+x^{13}+x^{15}+x^{16}$	$1+x+x^3+x^4$ $+x^8+x^{10}+x^{13}+x^{16}$
等冪生成式	$\sum_{i\in Q}x^i$	$\sum_{i\in N}x^i$	$1+\sum_{i\in Q}x^i$	$1+\sum_{i\in N}x^i$
維數	16	16	15	15
等價關係	Q_2	Q_1	Q'_2	Q'_1
對偶碼 $Q^{\perp}$	Q'_1	Q'_2	Q_1	Q_2
參數[n,k,d]	[31,16,7]	[31,16,7]	[31,15,8]	[31,15,8]

例 3：p=23≡-1 (mod 8)。Q={1,2,3,4,6,8,9,12,13,16,18}，
N={5,7,10,11,14,15,17,19,20,21,22}，四個二元 QR 碼 Q_1，Q_2，Q'_1，Q'_2 分別如下：其中 Q_1，Q_2 分別有參數 [23,12,7]，由 Golay 碼的唯一性，Q_1，Q_2 與 Golay 碼 G_{23} 等價，即 G_{23} 也是 QR 碼。

	Q_1	Q_2	Q'_1	Q'_2
生成多項式	$g_1(x)=1+x+x^5+x^6$ $+x^7+x^9+x^{11}$	$g_2(x)=1+x^2+x^4+x^5$ $+x^6+x^{10}+x^{11}$	$g_3(x)=1+x+x^2+x^3$ $+x^4+x^7+x^{10}+x^{12}$	$g_4(x)=1+x^2+x^5+x^8$ $+x^9+x^{10}+x^{11}+x^{12}$
等冪生成式	$\sum_{i\in Q}x^i=$ $g_1(x)(x+x^3+x^7)$	$\sum_{i\in N}x^i=$ $g_2(x)(x^5+x^9+x^{11})$	$1+\sum_{i\in Q}x^i=$ $g_3(x)(1+x^6)$	$1+\sum_{i\in N}x^i=$ $g_4(x)(1+x^2+x^4+x^6+x^{10})$
維數	12	12	11	11
等價關係	Q_2	Q_1	Q'_2	Q'_1
自正交	X	X	∨	∨
參數[n,k,d]	[23,12,7]	[23,12,7]	[23,11]	[23,11]

引理 2：質數 p ≡ 1 (mod 8)，Q，N，q(x)，n(x)，α如引理 1，有特性
(i)q*(x)為 q(x)的常數倍。
(ii)n*(x)為 n(x)的常數倍。
證明:稱幅有限不在此證明。

定理 4： 質數 p ≡ 1 (mod 8)，Q，N，q(x)，n(x)，α，Q_1，Q_2，Q'_1，Q'_2 的定義如前，則
(i)dim Q_1= dim Q_2= {p+1}/2。 dim Q'_1= dim Q'_2= {p-1}/2。
(ii)Q_1= Q'_1+< h(x)>， Q_2= Q'_2+< h(x)>， $Q_1\cap Q_2$=< h(x)>，且

$Q_1+Q_2=Rp=GF(l)[x])/<x^p-1>$。
(iii) $Q'_1 \cap Q'_2=\{0\}$，$Q'_1+Q'_2=\{Rp$ 中所有似偶向量$\}$。
(iv) $Q_1 \sim Q_2$，$Q'_1 \sim Q'_2$。
(v) $Q^{\perp}_1=Q'_2$，$Q^{\perp}_2=Q'_1$。
(vi)$d^2 \geq p$，其中 d 是 Q_1，Q_2 的最小加權值。
證明：(i)(ii)(iii)(iv)(vi)證明與定理 3 同。(v)的證明與定理 3 的(v)類似。唯一不同的是本定理需要應用引理 2 非引理 1。

推論 3：若 $l=2$，且質數 $p \equiv 1 \pmod 8$。Q_1，Q_2，Q'_1，Q'_2 分別有等冪生成式 $1+\sum_{i\in Q} x^i$ ，$1+\sum_{i\in N} x^i$ ，$\sum_{i\in N} x^i$ ，$\sum_{i\in Q} x^i$ 。

定理 5：[2, Thm69, p87] Q_1，Q_2 的擴充碼 $\underline{Q}_1$，$\underline{Q}_2$ 參數都是 $[p+1,(p+1)/2]$。
若 $p \equiv -1 \pmod 8$，$\underline{Q}_1$ 與 $\underline{Q}_2$ 是雙重對偶碼(即元素加權值是 4 的倍數且 $\underline{Q}^{\perp}=\underline{Q}$。
若 $p \equiv 1 \pmod 8$，$\underline{Q}_1^{\perp}=\underline{Q}_2$，$\underline{Q}_2^{\perp}=\underline{Q}_1$ 且 $\underline{Q}_1$，$\underline{Q}_2$ 是似偶電碼。

參、 結構(u，v)與結構(u，u+v) 的特性與其連接碼

在 1964 年， Plotkin [3]首先提出結構(u,u+v)的構想， 接著在 1970 年有 Sloane 與 Whitehead [4]做更深入的研究。對於以上兩種結構的特性可參考[5]。連接碼的種類很多, 隨著所選擇不同的連接結構與電碼，合成不同特性的連接碼。在此我們僅提出 2 種不同的結構方式(u，v)與(u，u+v)，來探討它所對應連接碼。

(I)結構 (u，v)：設 C_1,C_2 分別為 $[n_1,k_1,d_1]$ 電碼，$[n_2,k_2,d_2]$ 電碼，若 $C=\{(u,v):u\in C_1,v\in C_2\}$，則稱 C 為 C_1，C_2 對應結構 (u，v) 的連接碼。

例 4：若 $C_1=\{1011,0101,1110,0000\}$，$C_2=\{1010,0101,1111,0000\}$，且 $C=\{(u,v): u\in C_1,v\in C_2\}$，則 C 的元素如下:

(表一) $C=\{(u,v):u\in C_1,v\in C_2\}$ 的元素

u \ v	1010	0101	1111	0000
1011	10111010	10110101	10111111	10110000
0101	01011010	01010101	01011111	01010000
1110	11100101	11100101	11101111	11100000
0000	00001010	00000101	00001111	00000000

(II) 結構(u,u+v)：若 $C_1=[n_1,k_1,d_1]$，$C_2=[n_2,k_2,d_2]$，且 $C=\{(u,u+v):u\in C_1,v\in C_2\}$，則稱 C 為 C_1，C_2 對應結構(u,u+v)的連接碼。

定理 6[5]：$C=[n_1+\max\{n_1,n_2\}, k_1+k_2,d]$電碼，其中 $d=\min\{2d_1,d_2\}$。

此連接碼 C 的最小加權值 d 比結構(u,v) 所建立連接碼的最小加權值 d 顯著的大，因

此結構(u,u+v)在一般情況下比結構(u,v)實用。

定理 7：若 $C_1=[n,k_1]$碼， $C_2=[n,k_2]$碼，且 $C=\{(u,u+v): u\in C_1, v\in C_2\}$，
則 $C^{\perp}=\{(a+b,b): a\in C_1^{\perp}, b\in C_2^{\perp}\}$ 且 $C^{\perp}=[2n,2n-(k_1+k_2)]$碼。
事實上所有的 Reed-Muller 碼都可以用結構(u,u+v)建立。

肆、 對應連接結構(u,v), (u,u+v)的編碼與解碼

(I) 結構(u,v)

設 C_1，C_2 分別為 $[n_1,k_1,d_1]$，$[n_2,k_2,d_2]$ 電碼，且有生成矩陣(generator matrices)分別為 $G_1=[T_1|I_{k1}]_{k1xn1}\}$，$G_2=[T_2|I_{k2}]_{k2xn2}\}$，其中 I_k 表 kxk 的單位矩陣，且 T_1 表 $k_1x(n_1-k_1)$，T_2 表 $k_2x(n_2-k_2)$矩陣。若 $C=\{(u,v):u\in C_1, v\in C_2\}$，則對應電碼 C 的生成矩陣

$G=\begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}_{(k_1+k_2)x(n_1+n_2)}$，且 $C=[n_1+n_2,k_1+k_2,\min\{d_1,d_2\}]$電碼。

i) 編碼：令 $a=(a_1,a_2,..,a_{k1},a_{k1+1},\ldots a_{k1+k2})$表送方送出經轉換過的二元數位序列(binary digital sequence)。先將$(a_1,a_2,\ldots,a_{k1})$送進對應 C_1 的編碼器(encoder)，得到字元碼 u。再將$(a_{k1+1},\ldots,a_{k1+k2})$送進對應 C_2 的編碼器，得到字元碼 v。則(u,v)即是 a 經編碼後在 C 上的字元碼。u,v 的計算如下：

$u=(a_1,a_2,\ldots,a_{k1})\cdot G_1$，$v=(a_{k1+1},\ldots,a_{k1+k2})\cdot G_2$。

ii) 解碼：已知電碼 C 的最小加權值 $d=\min\{d_1,d_2\}$，所以假設有 q 個錯誤發生，其中 q 必須$\le\left\lfloor\frac{d-1}{2}\right\rfloor$。

假設有一個字元碼 $(u,v)\in C$ 被送出，收方收到的接收碼(received code)為 $r=(r_1,r_2,\ldots,r_{n1+n2})$。把 $(r_1,r_2,\ldots,r_{n1})$送進對應 C_1 的解碼器(decoder)中，$(r_{n1+1},\ldots,r_{n1+n2})$送進對應 C_2 的解碼器中。若在兩個解碼器中分別發現 q_1，q_2 個錯誤，則因

$q_1=<q\le\left\lfloor\frac{d-1}{2}\right\rfloor\le\left\lfloor\frac{d_1-1}{2}\right\rfloor$且 $q_2=<q\le\left\lfloor\frac{d-1}{2}\right\rfloor\le\left\lfloor\frac{d_2-1}{2}\right\rfloor$，因此兩個解碼器可完全正確的解碼。若說分別找出的錯誤是 e_1，e_2，則送出的字元碼必是 $r+(e_1,e_2)$。

(II) 結構(u,u+v)

設 C_1，C_2 分別為 $[n_1,k_1,d_1]$，$[n_2,k_2,d_2]$ 電碼，且有生成矩陣分別為 $G_1=[T_1|I_{k1}]_{k1xn1}$，$G_2=[T_2|I_{k2}]_{k2xn2}$，其中 I_k 表 kxk 的單位矩陣。為了簡化且不失一般性，以下我們假設 $n_1=n_2=n$。若 $C=\{(u,u+v): u\in C_1, v\in C_2\}$，則有生成矩陣 $G=\begin{bmatrix} G_1 & 0 \\ 0 & G_1+G_2 \end{bmatrix}_{(k_1+k_2)x(n_1+n_2)}$

且 C=[2n,k_1+k_2,min{$2d_1,d_2$}]電碼。

i) 編碼: 令 a=($a_1,a_2,..,a_{k1},a_{k1+1},\ldots a_{k1+k2}$)表送方送出經轉換過的二元數位序列。先將($a_1,a_2,\ldots,a_{k1}$)送進對應 C_1 的編碼器，得到字元碼 u。再將($a_{k1+1},\ldots,a_{k1+k2}$)送進對應 C_2 的編碼器，得到字元碼 v。則(u,u+v)即是 a 經編碼後在 C 上的字元碼。u，v 的計算方式與結構(u,v)同。

ii) 解碼:電碼 C 的最小加權值 d=min{$2d_1,d_2$}，所以假設在傳送時最多有 q 個錯誤發生，其中 $q\le\left\lfloor\frac{d-1}{2}\right\rfloor$。

假設有一個字元碼 (u,u+v) ∈C 被送出,收方收到的接收碼為 r=($r_1,r_2,\ldots,r_{n1+n2}$)。同結構(u,v)的解碼步驟，把 ($r_1,r_2,\ldots,r_{n1}$)送進對應 C_1 的解碼器(decoder)中，($r_{n1+1},\ldots,r_{n1+n2}$)送進對應 C_2 的解碼器中。若在兩個解碼器中分別發現 q_1，q_2 個錯誤，則 $q_1\le\left\lfloor\frac{d_1-1}{2}\right\rfloor$ 或 $q_2\le\left\lfloor\frac{d_2-1}{2}\right\rfloor$，否則 $q_1>\left\lfloor\frac{d_1-1}{2}\right\rfloor+1$ 且 $q_2>\left\lfloor\frac{d_2-1}{2}\right\rfloor+1$。但 $q=q_1+q_2>\left\lfloor\frac{d_1-1}{2}\right\rfloor+\left\lfloor\frac{d_2-1}{2}\right\rfloor+2>\left\lfloor\frac{d-1}{2}\right\rfloor$，此與 q 的假設不合。因此 $q_1\le\left\lfloor\frac{d_1-1}{2}\right\rfloor$ 或 $q_2\le\left\lfloor\frac{d_2-1}{2}\right\rfloor$。若說 $q_i\le\left\lfloor\frac{d_i-1}{2},\right\rfloor\ i=1,2$，即對應 C_i 的解碼器可正確的解碼。剩餘的部份做法與結構(u,v)類似，並請參考[6]。

伍、結論

在建立一個[n, k, d]電碼時, 我們希望

(1)當 $n\to\infty$ 時 k/n>> 0(即 k/n 不要太小)，碼字元才不會太少, 在編解碼時實用性才高。

(2) d 越大越好，確保該電碼的除錯能力。

在本文中, 我們所探討的 QR 碼皆符合以上兩個特性，因此 QR 碼在通訊上廣為專家使用。它也有很好的數學特性與結構[7, 8]，有不少學者在其上做許多研究。在前一部份所建立的新連接碼，不需重新發展一套長而複雜的裝備，只要應用現有的編解碼理論即可。作者已着手下一篇文章，將會更深入探討其應用。

陸、 參考文獻

[1]MacWilliams, T.J., Sloane, N.J.A., The theory of Error--Correcting Codes,North--Holland, Amsterdam(1979).

[2]Pless, V., Introduction to the Theory of Error--Correcting Codes, Wiley,New York (1982).
[3]Plotkin, M., “Binary code with specified minimum distances,” IEEE Trans. Info.Theory, 6, 445--450(1960).
[4]Sloane, N.J.A. and Whitehead, D.S.,”A new family of single--error--correcting code,”IEEE Trans. Info. Theory, 16, 717--719(1970).
[5]葉蘭英，“連接電碼的建立與其特性的探討，”技術學刊，Vol. 10， No. 4，53--59 (1995).
[6] N.J.A. Sloane, S.M. Reddy and C.L. Chen, “New Binary Codes,” IEEE Trans. Inform. Theory, 18(1972), 503--510.
[7]Mei Hui Chiu, Stephen S.-T. Yau, Yung Yu, “Z_8-Cycli Codes and Quadratic Residue Codes,” Advances in Applied Mathematics 25,12-33(2000)
[8]V. Pless and Z. Qian, “Cycli Codes and Quadratic Residue Codes over Z_4,” IEEE Trans. Inform. Theory 42, No. 5(1996),1594-1600.

柒、 致謝

本文為國科會計畫，計畫編號：NSC 93－2115－M－168－002，特在此致謝。

Investigation of Properties of Quadratic Residual Codes on Concatenated Structure

Larn-Ying Yeh

Department of Electronic Engineering , Kun Shan University Assistant Professor

ABSTRACT

This paper wants to apply Quadratic Residue Codes with structure (u,v) and structure (u,u+v), to establish new concatenated codes. Firstly, introducing the symbols and definitions for what be used in this paper, then investing the properties of Quadratic Residue Codes. Secondly, discussing their properties of the structures (u,v), (u,u+v). Finally, giving the method of designs of encoders and decoders for these concatenated codes .

Keywords: Quadratic Residue Code, Concatenated Structure, Concatenated Code, Cyclotomic coset