Codici ciclici

Codici ciclici - Definizione

- Dato il vettore $\mathbf{v} = [v_0, v_1, \ldots, v_{n-1}] \in \mathcal{V} = \mathrm{GF}(2)^n$ indichiamo con $\mathbf{v}^{(i)}$ il vettore ottenuto da $\mathbf{v}$ applicando uno shift ciclico di i posizioni a destra

$$\mathbf{v}^{(i)} = [v_{n-i}, v_{n-i+1}, \ldots, v_{n-1}, v_0, v_1, \ldots, v_{n-i-1}]$$

- Un codice lineare $\mathcal{C}(k, n)$ si definisce *ciclico* se data una generica parola di codice $\mathbf{x} \in \mathcal{C}(k, n)$ ogni suo shift ciclico $\mathbf{x}^{(i)}$ è ancora una parola di codice, $\mathbf{x}^{(i)} \in \mathcal{C}(k, n)$.

Codici ciclici - Esempi

- $\mathcal{C}(2,3) = \{000, 110, 101, 011\}$
- $\mathcal{C}(2,4) = \{0000, 1010, 0101, 1111\}$
- Il codice $\mathcal{C}(4,7)$

Message	Code vector	Polynomial
(0000)	0000000	$0 = 0 \cdot g(D)$
(1000)	1101000	$1 + D + D^3 = 1 \cdot g(D)$
(0100)	0110100	$D + D^2 + D^4 = D \cdot g(D)$
(1100)	1011100	$1 + D^2 + D^3 + D^4 = (1 + D) \cdot g(D)$
(0010)	0011010	$D^2 + D^3 + D^5 = D^2 \cdot g(D)$
(1010)	1110010	$1 + D + D^2 + D^5 = (1 + D^2) \cdot g(D)$
(0110)	0101110	$D + D^3 + D^4 + D^5 = (D + D^2) \cdot g(D)$
(1110)	1000110	$1 + D^4 + D^5 = (1 + D + D^2) \cdot g(D)$
(0001)	0001101	$D^3 + D^4 + D^6 = D^3 \cdot g(D)$
(1001)	1100101	$1 + D + D^4 + D^6 = (1 + D^3) \cdot g(D)$
(0101)	0111001	$D + D^2 + D^3 + D^6 = (D + D^3) \cdot g(D)$
(1101)	1010001	$1 + D^2 + D^6 = (1 + D + D^3) \cdot g(D)$
(0011)	0010111	$D^2 + D^4 + D^5 + D^6 = (D^2 + D^3) \cdot g(D)$
(1011)	1111111	$1 + D + D^2 + D^3 + D^4 + D^5 + D^6 = (1 + D^2 + D^3) \cdot g(D)$
(1111)	1001011	$1 + D^3 + D^5 + D^6 = (1 + D + D^2 + D^3) \cdot g(D)$

Rappresentazione algebrica di un codice ciclico

- A ciascun vettore $\mathbf{v} = [v_0, v_1, \ldots, v_{n-1}] \in \mathcal{V}$ è possibile associare un polinomio definito in GF(2),

$$v(D) = v_0 + v_1 D + \cdots + v_{n-1} D^{n-1},$$

$$\mathbf{v} \leftrightarrow v(D).$$

- *Definizione*. Se $x(D) \leftrightarrow \mathbf{x} \in \mathcal{C}(k, n) \implies$ si dice che $x(D)$ è in $\mathcal{C}(k, n)$.
- *Proprietà*. Uno shift ciclico di i posizioni del vettore $\mathbf{v}$ è equivalente a moltiplicare il polinomio $v(D)$ per D^i modulo $(D^n - 1)$

$$\mathbf{v}^{(i)} \leftrightarrow \quad \text{mod } \{D^i v(D), (D^n - 1)\}.$$

Rappresentazione algebrica di un codice ciclico

Ad esempio, fissando $i = 1$, il polinomio diventa

$$\begin{aligned} Dv(D) &= v_0 D + v_1 D^2 + \cdots + v_{n-1} D^n \\ &= v_{n-1} + v_0 D + v_1 D^2 + \cdots + v_{n-2} D^{n-1} + v_{n-1} D^n - v_{n-1} \\ &= v_{n-1} + v_0 D + v_1 D^2 + \cdots + v_{n-2} D^{n-1} + v_{n-1}(D^n - 1) \end{aligned}$$

In questo caso si ha

$$\text{mod } \{Dv(D), (D^n - 1)\} = v_{n-1} + v_0 D + v_1 D^2 + \cdots + v_{n-2} D^{n-1} \leftrightarrow \mathbf{v}^{(1)}$$

Analogamente, si può mostrare che

$$D^i v(D) = q(D)(D^n - 1) + v_{n-i} + v_{n-i+1} D + \cdots + v_{n-i-1} D^{n-1},$$

e quindi

$$\text{mod } \{D^i v(D), (D^n - 1)\} \leftrightarrow \mathbf{v}^{(i)}$$

Rappresentazione algebrica di un codice ciclico

Terorema. Sia $g(D) = g_0 + g_1 D + \cdots + g_r D^r$ il polinomio di grado minimo associato ad una parola del codice ciclico $\mathcal{C}(k, n) \implies$ a) $g_0 = 1$, e b) $g(D)$ è unico.
Dimostrazione.

a) Supponiamo *per assurdo* che $g_0 = 0 \implies$

$$\begin{aligned} g(D) &= g_1 D + g_2 D^2 + \cdots + g_r D^r \\ &= D\left(g_1 + g_2 D + \cdots + g_r D^{r-1}\right) = D g'(D) \end{aligned}$$

ma questo contraddice le ipotesi poiché $\mathcal{C}(k, n)$ è ciclico e quindi $g'(D)$ è in $\mathcal{C}(k, n)$ ma il grado di $g'(D)$ è minore di r. Un ragionamento simile si può fare per $g_r = 0$.

b) Supponiamo che esistano *due* polinomi di grado minimo $g_1(D)$ e $g_2(D)$ in $\mathcal{C}(k, n) \implies g_3(D) = g_1(D) - g_2(D)$ è ancora in $\mathcal{C}(k, n)$ e per quanto visto nella parte a) il grado di $g_3(D)$ sarebbe minore di r. Impossibile.

Polinomio generatore di un codice ciclico

Definizione. Il *polinomio generatore* di un codice ciclico $\mathcal{C}(k, n)$ è il polinomio

$$g(D) = 1 + g_1 D + \cdots + D^r,$$

non nullo e di grado minimo in $\mathcal{C}(k, n)$.

Codici ciclici - Esempi

- $\mathcal{C}(2,3) = \{000, 110, 101, 011\} \implies g(D) = 1 + D$
- $\mathcal{C}(2,4) = \{0000, 1010, 0101, 1111\} \implies g(D) = 1 + D^2$
- Il codice $\mathcal{C}(4,7) \implies g(D) = 1 + D + D^3$

Message	Code vector	Polynomial
(0000)	0000000	$0 = 0 \cdot g(D)$
(1000)	1101000	$1 + D + D^3 = 1 \cdot g(D)$
(0100)	0110100	$D + D^2 + D^4 = D \cdot g(D)$
(1100)	1011100	$1 + D^2 + D^3 + D^4 = (1 + D) \cdot g(D)$
(0010)	0011010	$D^2 + D^3 + D^5 = D^2 \cdot g(D)$
(1010)	1110010	$1 + D + D^2 + D^5 = (1 + D^2) \cdot g(D)$
(0110)	0101110	$D + D^3 + D^4 + D^5 = (D + D^2) \cdot g(D)$
(1110)	1000110	$1 + D^4 + D^5 = (1 + D + D^2) \cdot g(D)$
(0001)	0001101	$D^3 + D^4 + D^6 = D^3 \cdot g(D)$
(1001)	1100101	$1 + D + D^4 + D^6 = (1 + D^3) \cdot g(D)$
(0101)	0111001	$D + D^2 + D^3 + D^6 = (D + D^3) \cdot g(D)$
(1101)	1010001	$1 + D^2 + D^6 = (1 + D + D^3) \cdot g(D)$
(0011)	0010111	$D^2 + D^4 + D^5 + D^6 = (D^2 + D^3) \cdot g(D)$
(1011)	1111111	$1 + D + D^2 + D^3 + D^4 + D^5 + D^6 = (1 + D^2 + D^3) \cdot g(D)$
(1111)	1001011	$1 + D^3 + D^5 + D^6 = (1 + D + D^2 + D^3) \cdot g(D)$

Polinomio generatore di un codice ciclico

Teorema. Un polinomio $x(D)$ è in $\mathcal{C}(k,n) \iff x(D)$ è un multiplo di $g(D)$.
Dimostrazione.

a) Ogni multiplo di $g(D)$ è in $\mathcal{C}(k,n)$. Poiché $\mathcal{C}(k,n)$ è ciclico i polinomi $Dg(D), D^2g(D), \ldots, D^{n-r-1}g(D)$ sono in $\mathcal{C}(k,n)$ e lo è anche qualsiasi loro combinazione lineare $x(D) = u(D)g(D) = u_0g(D) + u_1Dg(D) + \cdots + u_{n-r-1}D^{n-r-1}g(D)$.

b) Ogni polinomio in $\mathcal{C}(k,n)$ può essere espresso come multiplo di $g(D)$. Per *assurdo* assumiamo che $x(D)$ sia in $\mathcal{C}(k,n)$ ma non un multiplo di $g(D) \implies x(D) = a(D)g(D) + b(D)$, $b(D) = x(D) - a(D)g(D)$. Poichè sia $x(D)$ che $a(D)g(D)$ sono in $\mathcal{C}(k,n)$, per la linearità del codice anche $b(D)$ è in $\mathcal{C}(k,n)$ ma questo è impossibile perché $b(D)$, essendo il resto alla divisione di $x(D)$ per $g(D)$, è di grado minore di $g(D)$.

Polinomio generatore di un codice ciclico

Corollario 1. L'insieme degli $n - r$ polinomi

$$\{g(D), Dg(D), D^2 g(D), \ldots, D^{n-r-1} g(D)\}$$

costituisce una base per $\mathcal{C}(k, n)$.
Corollario 2. Se il polinomio generatore $g(D)$ del codice $\mathcal{C}(k, n)$ ha grado $r \implies$ il numero di parole del codice è 2^{n-r} e $r = n - k$.
Dimostrazione. Tutte le possibili combinazioni in GF(2) degli $n - r$ polinomi che costituiscono una base per $\mathcal{C}(k, n)$ sono 2^{n-r} e quindi le parole di codice sono $2^{n-r} \implies k = n - r$ e $r = n - k$.
Corollario 3. Il grado del polinomio generatore $g(D)$ del codice $\mathcal{C}(k, n)$ è uguale al numero di bit di controllo di parità.

Teorema fondamentale generatore di un codice ciclico

Teorema. Un polinomio $g(D)$ è generatore di un codice ciclico $\mathcal{C}(k,n) \iff g(D)$ è un divisore di $D^n - 1$.
Dimostrazione.

a) Il polinomio $g(D)$ è generatore di $\mathcal{C}(k,n) \implies g(D)$ è un divisore di $D^n - 1$.
Poiché $g(D)$ è di grado $n-k$, si ha che

$$D^k g(D) = (D^n - 1) + g^{(k)}(D),$$

da cui

$$(D^n - 1) = D^k g(D) - g^{(k)}(D) = \Big(D^k - a(D)\Big)\, g(D)$$

Teorema fondamentale generatore di un codice ciclico

b) Se il polinomio $g(D)$ di grado $n-k$ è un divisore di $D^n-1 \implies g(D)$ è generatore di un codice ciclico $\mathcal{C}(k,n)$.
Qualsiasi polinomio della forma

$$x(D) = u_0 g(D) + u_1 D g(D) + \cdots + u_{k-1} D^{k-1} g(D) = u(D) g(D)$$

ha grado pari o inferiore a $n-1$ ed è un multiplo di $g(D)$.
Poichè $u(D)$ può assumere 2^k valori $\implies$ l'insieme dei 2^k vettori forma un codice lineare $\mathcal{C}(k,n)$.
Sia $v(D) = v_0 + v_1 D + \cdots + v_{n-1} D^{n-1} = a(D) g(D)$ in $\mathcal{C}(k,n) \implies$

$$\begin{aligned} Dv(D) &= v_0 D + v_1 D^2 + \cdots + v_{n-1} D^n \\ &= v_{n-1}(D^n - 1) + \left(v_{n-1} + v_0 D + \cdots + v_{n-2} D^{n-1}\right) \\ &= v_{n-1}(D^n - 1) + v^{(1)}(D) \end{aligned}$$

Poichè $g(D)$ è divisore di D^n-1 (per ipotesi) e di $Dv(D) = Da(D)g(D)$ anche $v^{(1)}(D)$ è un multiplo di $g(D)$ $\implies \mathcal{C}(k,n)$ è ciclico.

Divisione tra polinomi in GF(2) - Esempi

- $\mathcal{C}(2,3) = \{000, 110, 101, 011\} \implies g(D) = 1 + D.$

$$(D^3 - 1)/(1 + D) = D^2 + D + 1.$$

- $\mathcal{C}(2,4) = \{0000, 1010, 0101, 1111\} \implies g(D) = 1 + D^2$

$$(D^4 - 1)/(1 + D^2) = D^2 + 1.$$

- Il codice $\mathcal{C}(4,7) \implies g(D) = 1 + D + D^3$

$$(D^7 - 1)/(1 + D + D^3) = D^4 + D^2 + D + 1.$$

- Il polinomio $D^6 - 1$ può essere fattorizzato in molte maniere diverse. Ad ogni fattore corrisponde un polinomio generatore $g(D)$ diverso e quindi un codice ciclico diverso.

$$(D^6 - 1) = (1 + D^2)^2(1 + D + D^2)^2.$$

Matrice generatrice di un codice ciclico

Dato il codice ciclico $\mathcal{C}(k, n)$ con polinomio generatore $g(D)$, dal momento che l'insieme dei polinomi

$$\{g(D), Dg(D), D^2g(D), \ldots, D^{k-1}g(D)\}$$

costituisce una base per il codice, la matrice generatrice del codice è

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & \cdots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}$$

Considerato che $g_0 = 1$, le righe possono essere sommate tra loro per ottenere la matrice generatrice del codice equivalente in forma sistematica.

Controllo di parità per un codice ciclico

Dato il codice ciclico $\mathcal{C}(k, n)$ con polinomio generatore $g(D)$, esiste sempre un polinomio $h(D) = h_0 + h_1 D + \cdots + h(k)D^k$ tale che

$$h(D) = (D^n - 1)/g(D) \implies g(D)h(D) = D^n - 1.$$

- Sia $x(D) = u(D)g(D)$ in $\mathcal{C}(k, n)$ $\implies$

$$\begin{aligned} v(D) &= x(D)h(D) = u(D)g(D)h(D) \\ &= u(D)(D^n - 1) = D^n u(D) - u(D). \end{aligned}$$

- Poiché $u(D)$ è un polinomio di grado massimo $k - 1$ e $D^n u(D)$ è di grado minimo n, sappiamo per certo che, se $x(D)$ è in $\mathcal{C}(k, n)$, gli $n - k$ coefficienti con indici $k, k + 1, \ldots, n - 1$ del polinomio $v(D)$ devono essere 0.

Controllo di parità per un codice ciclico

- Poiché è $v(D) = x(D)h(D)$, il coefficiente m-esimo del polinomio $v(D)$ si ottiene come la somma di tutti i coefficienti che moltiplicano D^m

$$v_m = x_0 h_m + x_1 h_{m-1} + \cdots + x_m h_0 = \sum_{j=0}^{n-1} x(j)h(m-j).$$

- Abbiamo un set di $n-k$ equazioni del tipo

$$v_m = \sum_{j=0}^{n-1} x(j)h(m-j) = 0, \quad m = k, k+1, \ldots, n-1.$$

Controllo di parità per un codice ciclico

- Le $n-k$ equazioni possono essere riassunte in forma matriciale

$$\mathbf{x}\mathbf{H}^T = \mathbf{0}_{n-k}.$$

dove la matrice $\mathbf{H}$, di dimensioni $(n-k) \times n$, è la matrice di controllo di parità del codice ciclico $\mathcal{C}(k, n)$.

$$\mathbf{H}^T = \begin{bmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 \end{bmatrix}$$

- La sindrome può essere calcolata come

$$\mathbf{s} = \mathbf{y}\mathbf{H}^T$$

Esempio di calcolo di matrice generatrice e di controllo di parità

Dato il codice ciclico $\mathcal{C}(k = 4, n = 7)$ con polinomio generatore $g(D) = 1 + D + D^3$, la matrice generatrice è

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

ed in forma sistematica diventa

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Esempio di calcolo di matrice generatrice e di controllo di parità

Dato il codice ciclico $\mathcal{C}(k = 4, n = 7)$ con polinomio generatore $g(D) = 1 + D + D^3$, il vettore $h(D) = (D^n - 1)/g(D) = 1 + D + D^2 + D^4$. I coefficienti del polinomio sono $h_0 = 1, h_1 = 1, h_2 = 1, h_3 = 0, h_4 = 1$ e la matrice di controllo di parità è

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

ed in forma sistematica diventa

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Metodo alternativo per il calcolo della sindrome

La sindrome associata alla matrice di controllo di parità sistematica si può calcolare usando un metodo alternativo.
Al ricevitore si ha

$$\mathbf{y} = \mathbf{x} + \mathbf{e} \implies y(D) = x(D) + e(D)$$

La sindrome di $\mathbf{y}$ può essere calcolata come il resto della divisione tra polinomi $y(D)/g(D) \implies y(D) = a(D)g(D) + s(D)$.

Metodo alternativo per il calcolo della sindrome

Poiché il grado di $s(D)$ è *minore* del grado di $g(D)$, il grado massimo di $s(D)$ è $n-k-1$.

- Se è $e(D)=0$, il canale non introduce errori ed è

$$s(D) = \mathrm{mod}\,\{x(D), g(D)\} = \mathrm{mod}\,\{u(D)g(D), g(D)\} = 0$$

- Se è $e(D)\neq 0$, la sindrome è

$$\begin{aligned} s(D) &= \mathrm{mod}\,\{x(D)+e(D), g(D)\} \\ &= \mathrm{mod}\,\{x(D), g(D)\} + \mathrm{mod}\,\{e(D), g(D)\} \\ &= \mathrm{mod}\,\{e(D), g(D)\} \end{aligned}$$

- $s(D)$ corrispone alla sindrome ottenuta con la matrice di controllo di parità in forma *sistematica*.

Decodifica a sindrome per codici ciclici

Ci sono due metodi possibili per effettuare la decodifica dei codici ciclici:

1. Approccio classico codici a blocco: La sindrome $s(D)$ mappa un polinomio di grado $n-1$ su uno di grado $n-k-1$. Una volta calcolata la sindrome, si identifica un coset ed il pattern di errore corrisponde al coset leader. *Svantaggio*: la complessità di associare tutti i vettori in $\mathcal{V}$ ad uno specifico coset.
2. Sfruttare le proprietà dei codici ciclici per derivare un metodo alternativo.

Decodifica a sindrome per codici ciclici

Teorema. Dato il codice ciclico $\mathcal{C}(k, n)$ con polinomio generatore $g(D)$ e distanza minima d_{min}, sia $s(D)$ la sindrome associata al vettore ricevuto $\mathbf{y}$, se $w(s(D)) \leq \lfloor \frac{d_{min}-1}{2} \rfloor \implies \hat{e}(D) = s(D)$.
Dimostrazione. Per costruzione $s(D)$ e $y(D)$ sono nello stesso coset $C_y = C_s = \{\mathcal{C} + s(D)\}$, poiché si ha $w(\mathbf{s}) \leq \lfloor \frac{d_{min}-1}{2} \rfloor \implies s(D) \leftrightarrow [\mathbf{s}, 0 \ldots, 0]$ è il coset leader e quindi la stima dell'errore.
In altre parole, poiché $s(D) = \mathrm{mod}\,\{e(D), g(D)\}$, se il grado di $e(D) < n - k \implies s(D) = e(D)$.

Esempio di decodifica per codici ciclici

Sia $\mathbf{x} = [0110100]$ una parola del codice ciclico $\mathcal{C}(4,7)$ con polinomio generatore $g(D) = 1 + D + D^3$.

- Sia $\mathbf{e} = [0100000]$ l'errore introdotto dal canale. Il vettore ricevuto è $\mathbf{y} = \mathbf{x} + \mathbf{e} = [0010100] \leftrightarrow y(D) = D^2 + D^4$.

$$s(D) = \text{mod}\,\{y(D), g(D)\} = D$$

Poichè $w(s(D)) = 1 \implies s(D) = \hat{e}(D) \implies \hat{\mathbf{e}} = [0100000]$.

- Sia $\mathbf{e} = [0000010]$ l'errore introdotto dal canale. Il vettore ricevuto è $\mathbf{y} = \mathbf{x} + \mathbf{e} = [0110110] \leftrightarrow y(D) = D + D^2 + D^4 + D^5$.

$$s(D) = \text{mod}\,\{y(D), g(D)\} = D^2 + D + 1$$

Poichè $w(s(D)) = 3 \implies s(D) \neq \hat{e}(D)$ e per trovare l'errore bisogna trovare un altro metodo.

Decodifica a sindrome per codici ciclici

Teorema. Dato il codice ciclico $\mathcal{C}(k, n)$, sia $s(D)$ la sindrome del vettore ricevuto $\mathbf{y} \implies$ la sindrome $s_1(D)$ della parola $\mathbf{y}^{(1)}$ ottenuta dallo shift di ciclico di $\mathbf{y}$ di una posizione si calcola

$$s_1(D) = \text{mod}\left\{y^{(1)}(D), g(D)\right\} = Ds(D) - s_{n-k-1}g(D)$$

Dimostrazione. Poiché vale la relazione $y(D) = u(D)g(D) + s(D)$, la relazione relativa a $y^{(1)}(D)$ è

$$\begin{aligned} Dy(D) &= Du(D)g(D) + Ds(D) \\ &= \left(Du(D)g(D) + s_{n-k-1}\right) g(D) + Ds(D) - s_{n-k-1}g(D) \end{aligned}$$

Poiché il grado massimo di $Ds(D) - s_{n-k-1}g(D)$ è $n - k - 1 \implies s_1(D) = Ds(D) - s_{n-k-1}g(D)$ è il resto della divisione di $Dy(D)$ per $g(D)$ ed è quindi è la sindrome di $y^{(1)}(D)$.

Esempio di decodifica per codici ciclici

Sia $\mathbf{x} = [0110100]$ una parola del codice ciclico $\mathcal{C}(4,7)$ con polinomio generatore $g(D) = 1 + D + D^3$ ed $\mathbf{e} = [0000010]$ l'errore introdotto dal canale. Il vettore ricevuto è $\mathbf{y} = \mathbf{x} + \mathbf{e} = [0110110] \leftrightarrow y(D) = D + D^2 + D^4 + D^5$.

$$s(D) = \text{mod}\,\{y(D), g(D)\} = D^2 + D + 1.$$

Lo shift ciclico di $\mathbf{y}$ è $\mathbf{y}^{(1)} = [0011011] \leftrightarrow y^{(1)}(D) = D^2 + D^3 + D^5 + D^6$.

$$s_1(D) = \text{mod}\left\{y^{(1)}(D), g(D)\right\} = D^2+1 = D(D^2+D+1)-D^3+D+1.$$

Lo shift ciclico di $\mathbf{y}^{(1)}$ è $\mathbf{y}^{(2)} = [1001101] \leftrightarrow y^{(2)}(D) = 1 + D^3 + D^4 + D^6$.

$$s_2(D) = \text{mod}\left\{y^{(2)}(D), g(D)\right\} = 1 = D(D^2+1) - D^3 + D + 1.$$

Decodifica a sindrome per codici ciclici

Definizione. Dato un vettore $\mathbf{v}$ di n componenti, una *sequenza ciclica* di zeri di lunghezza ℓ è una successione di ℓ zeri consecutivi in senso ciclico.

Esempi

1. $n = 7$, $\ell = 3$, $\mathbf{v} = [1000101]$;
2. $n = 7$, $\ell = 4$, $\mathbf{v} = [0010100]$;
3. $n = 15$, $\ell = 9$, $\mathbf{v} = [000000110001000]$

Decodifica a sindrome per codici ciclici

Teorema. Dato il codice ciclico $\mathcal{C}(k, n)$, con polinomio generatore $g(D)$ e distanza minima d_{min}, tale che tutti i pattern di errore correggibili abbiano una *sequenza ciclica* di almeno k zeri, ricevuto il vettore $\mathbf{y} = \mathbf{x} + \mathbf{e}$ con $w(\mathbf{e}) \leq \lfloor \frac{d_{min}-1}{2} \rfloor$, l'algoritmo di decodifica a massima verosimiglianza è composto dai seguenti passi

1. Calcolo iterativamente le sindromi di $s_i(D)$ per tutti gli shift ciclici di $y(D)$ e computo $w(s_i(D))$;
2. Trovo m per cui $w(s_m(D)) \leq \lfloor \frac{d_{min}-1}{2} \rfloor$;
3. Stimo $\hat{e}(D) = \text{mod}\left\{D^{n-m}s_m(D), D^{n-1}\right\}$.

Decodifica a sindrome per codici ciclici

Dimostrazione.

1. *Esistenza di m*. Poichè $w(\mathbf{e}) \leq \lfloor \frac{d_{min}-1}{2} \rfloor$ e tutti i pattern di errore correggibili hanno una *sequenza ciclica* di almeno k zeri, esiste uno shift ciclico di m posizioni di $\mathbf{y}$ tale che tutti gli 1 di $\mathbf{e}$ siano compresi nelle prime $n-k$ posizioni di $\mathbf{y}^m \implies s_{m(D)} = e^{(m)}(D)$.
2. *Stima dell'errore*

$$\begin{aligned} D^m \left(y(D) + D^{n-m} s_m(D) \right) &= D^m y(D) + D^n s_m(D) \\ &= y^{(m)}(D) + D^n s_m(D) \\ &= u(D)g(D) + s_m(D) + D^n s_m(D) \\ &= u(D)g(D) + (D^n - 1)s_m(D) \\ &= (u(D) + h(D)s_m(D))g(D). \end{aligned}$$