

Lección 13: Codificación de Canal.

Parte III

Gianluca Cornetta, Ph.D.

Dep. de Ingeniería de Sistemas de Información y Telecomunicación

Universidad San Pablo-CEU



Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Contenido

- Utilidad de la Matriz Estándar
- Códigos Cíclicos
- Códigos de Hamming



Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Utilidad de la Matriz Estándar

- ❑ La matriz estándar es una herramienta muy potente que permite estudiar la capacidad de detección y corrección de un código de bloque lineal (n, k) incluso para códigos con n grande
- ❑ Un indicador de la capacidad de un código de detectar y corregir t errores es límite de Hamming (*Hamming bound*)
- ❑ El límite de Hamming permite establecer cuál es el mínimo número de bits de paridad o de filas de la matriz estándar necesarios para corregir todas las posibles combinaciones de t errores y es definido como:

$$\text{Number of parity bits: } n-k \geq \log_2 \left[1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{t} \right]$$

$$\text{Number of correctable errors: } 2^{n-k} > \left[1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{t} \right]$$

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Cartagena99

Utilidad de la Matriz Estándar

- ❑ La capacidad de detección y corrección de error de un código (n, k) depende de la distancia mínima d_{min} entre palabras y viceversa
- ❑ El número mínimo t de errores que se desea corregir determina pues la distancia de Hamming mínima del código d_{min} :

$$t = \frac{d_{min} - 1}{2} \Rightarrow d_{min} = 2t + 1$$

- ❑ El t mínimo deseable en $t=2$ lo que lleva a una distancia mínima $d_{min} = 5$
- ❑ Es deseable poder transmitir al menos 2 bits de dato por cada palabra de código (es decir, el código más sencillo debe ser de tipo $(n, 2)$ y tener pues $k=2$)

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Utilidad de la Matriz Estándar

- $k=t=2$ se utilizan para determinar el límite de Hamming mínimo

$$2^{n-2} \geq \left[1 + \binom{n}{1} + \binom{n}{2} \right]$$

- La desigualdad anterior se resuelve numéricamente encontrando que el valor mínimo de n que la satisface es $n=7$:

$$\begin{cases} \binom{7}{1} = \frac{7!}{1!(7-1)!} = 7 \\ \binom{7}{2} = \frac{7!}{2!(7-2)!} = 21 \end{cases} \Rightarrow 2^{7-2} = 32 \geq \left[1 + \binom{7}{1} + \binom{7}{2} \right] = [1 + 7 + 21] = 29$$

- Es deseable diseñar un código con n mínimo por cuestiones de eficiencia de banda y sencillez de implementación
- Por tanto el código de dimensiones mínimas es el (7, 2). La matriz generadora \mathbf{G} de este código está formada por $k=2$ 7-tuplas linealmente

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Utilidad de la Matriz Estándar

- Una posible matriz generadora del código (7, 2) es:

$$\mathbf{G} = \begin{bmatrix} \mathbf{V}_1 \\ \mathbf{V}_2 \end{bmatrix} = [\mathbf{P} \mid \mathbf{I}_2] = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- Es fácil verificar que las dos filas de \mathbf{G} forman una base del subespacio S de V_7 ya que $\mathbf{V}_1 + \mathbf{V}_2 \neq \{\mathbf{V}_1, \mathbf{V}_2\}$ y $\mathbf{V}_1 + \mathbf{V}_2 \in S$
- El código \mathbf{U}_2 relativo al mensaje $\mathbf{m}_2 = [0 \ 1]$ se calcula como:

$$\mathbf{U}_2 = \mathbf{m}_2 \mathbf{G} = [0 \ 1] \cdot \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = [0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1]$$

- Recordando que:

$$d_{\min} = \min \{w(\mathbf{U}_1), w(\mathbf{U}_2)\} = w(\mathbf{U}_2) = 3$$

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Cartagena99

Utilidad de la Matriz Estándar

- ❑ Por consiguiente el límite de Hamming no es una condición suficiente para el código (7, 2)
- ❑ Es necesario verificar el cumplimiento de otro límite que se denomina límite de Plotkin:

$$d_{\min} \leq \frac{n \times 2^{k-1}}{2^k - 1}$$

- ❑ En general un código de bloque lineal (n, k) debe cumplir con ambos límites con las siguientes diferencias:
 - ❑ Para códigos con relación de código k/n elevada, si el código cumple con el límite de Hamming entonces satisfará también el límite de Plotkin
 - ❑ Para códigos con relación de código k/n baja (como es el caso de este ejemplo), si el código cumple con el límite de Plotkin entonces satisfará también el límite de Hamming
- ❑ Por consiguiente el código más pequeño que asegura $d_{\min} = 5$ es el (8, 2)
- ❑ Obviamente se trata de un código realizable pero poco práctico debido a su

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Utilidad de la Matriz Estándar

- La matriz generadora del código (8, 2) es:

$$\mathbf{G} = [\mathbf{P} \mid \mathbf{I}_2] = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- La operación de detección empieza calculando el síndrome del código (n, k) , por ello es necesario determinar la transpuesta \mathbf{H}^T de la matriz de control de paridad \mathbf{H}
- \mathbf{H}^T es una matriz $n \times (n-k)$, por lo que para un código (8, 2) es:

$$\mathbf{H}^T = \begin{bmatrix} \mathbf{I}_6 \\ \mathbf{P} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

CLASES PARTICULARES, TUTORIAS TECNICAS ONLINE
LLAMA O ENVIA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Cartagena99

Utilidad de la Matriz Estándar

- ❑ El síndrome por cada uno de los posible 2^{n-k} patrones de error es $S_i = e_i H^T$, con $i=1, \dots, 2^{n-k}$
 - ❑ e_i representa el i -ésimo líder de *coset* (una fila de la matriz estándar), es decir, uno de los 2^{n-k} patrones de error que pueden perturbar todos los posibles 2^k códigos U_j del conjunto
- ❑ Utilizando esta ecuación se construye la tabla de síndromes que permite detectar el patrón de error que corresponde a un síndrome dado
- ❑ El patrón de error estimado se suma (módulo 2) al código corrompido recibido por el detector para calcular el código correcto
- ❑ Un código suele ser diseñado para corregir α errores y detectar simultáneamente β errores ($\beta \geq \alpha$) siempre que se cumpla la condición siguiente:

$$d_{\min} \geq \alpha + \beta + 1 \Rightarrow \alpha + \beta \leq d_{\min} - 1 = 5 - 1 = 4$$

- ❑ Por tanto existen las siguientes posibilidades:

<i>Detect</i> (α)	<i>Correct</i> (β)
2	2
3	1
4	0

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Cartagena99

Utilidad de la Matriz Estándar

- ❑ La detección es un proceso sencillo ya que un error es detectado si el síndrome del vector recibido es distinto de cero
- ❑ El proceso de corrección es más complejo ya que implica también detectar el patrón de error que ha generado un síndrome dado para poderlo corregir
- ❑ Este proceso equivale a realizar las siguientes operaciones (en el caso de nuestro código (8, 2)):

$$S_i = r_i H^T = [r_1 \ r_2 \ r_3 \ r_4 \ r_5 \ r_6 \ r_7 \ r_8] \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \Rightarrow \begin{cases} S_1 = r_1 + r_8 \\ S_2 = r_2 + r_8 \\ S_3 = r_3 + r_7 + r_8 \\ S_4 = r_4 + r_7 + r_8 \\ S_5 = r_5 + r_7 \end{cases}$$

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Utilidad de la Matriz Estándar

- ❑ La complejidad de la tabla de corrección depende del número de errores simultáneos (1 ó 2) que se desea corregir
- ❑ En el caso de corrección de error sencillo ($\beta=1$) el decodificador se diseña para evaluar sólo los primeros 9 *cosets* de la matriz estándar entre los 64 posibles
- ❑ En el caso de corrección hasta error dobles ($\beta=2$) el decodificador se diseña para evaluar sólo los primeros 37 *cosets* de la matriz estándar entre los 64 posibles
- ❑ Los *cosets* de 38 a 64 se utilizan para la corrección de un subconjunto de errores triples (26 de los 53 posibles). Estos *cosets* no se utilizan en decodificadores de distancia limitada (los cuales sólo corrigen hasta errores de orden t)
- ❑ Un código (n, k) diseñado para corregir errores hasta grado t no puede ser reorganizado para corregir sólo errores de tipo $t+1$, aunque la matriz estándar tenga el tamaño suficiente para contener todos los *cosets* relativos a estos tipo de error
 - ❑ El único parámetro que fija el máximo número de errores simultáneos errores es posible corregir es la distancia de Hamming mínima d_{min} ($d_{min}=5$ impone $t=2$)
 - ❑ Una secuencia de x bits erróneos sólo podría ser corregible si todos los vectores de peso x son líderes de *coset* (es decir, sólo aparecen en la primera columna de la matriz estándar), si un vector de peso x aparece en alguna otra columna el error no es corregible incluso si la matriz estándar tiene tamaño suficiente para contener todos los patrones de error de peso x

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Códigos Cíclicos

- ❑ Los códigos cíclicos binarios son una subclase muy importante de los códigos de bloque lineales
- ❑ Esta clase de códigos puede implementarse fácilmente utilizando un registro de desplazamiento realimentado lineal (*Linear Feedback Shift Register –LFSR*)
- ❑ El síndrome puede calcularse utilizando registros análogos
- ❑ Un código lineal es (n, k) es un código cíclico cuando se verifica la siguiente condición:
 - ❑ Si la n -tupla es un código $\mathbf{U}=(u_0, u_1, \dots, u_{n-1})$ en el subespacio $S \Rightarrow$ también $\mathbf{U}^{(1)}=(u_{n-1}, u_0, u_1, \dots, u_{n-2})$, obtenido rotando \mathbf{U} en sentido horario una única vez, pertenece a S
 - ❑ En general $\mathbf{U}^{(i)}=(u_{n-i}, u_{n-i+1}, \dots, u_{n-1}, u_0, u_1, \dots, u_{n-i-1})$, obtenido rotando \mathbf{U} en sentido horario i veces, todavía es un elemento de S
 - ❑ Los componentes de $\mathbf{U}=(u_0, u_1, \dots, u_{n-1})$ pueden considerarse como los coeficientes de un polinomio de grado $n - 1$:

$$\mathbf{U}(X) = u_0 + u_1 X + u_2 X^2 + \dots + u_{n-1} X^{n-1} \quad u_i = \{0,1\}$$

- ❑ En general, una n -tupla es descrita por un polinomio de grado menor o igual a

CLASES PARTICULARES, TUTORIAS TECNICAS ONLINE
LLAMA O ENVIA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Cartagena99

Códigos Cíclicos

- Si $U(X)$ es un polinomio de grado $n - 1 \Rightarrow U^{(i)}(X)$ es el resto de la división $X^i U(X)/(X^n + 1)$, es decir:

$$\frac{X^i U(X)}{X^n + 1} = q(X) + \frac{U^{(i)}(X)}{X^n + 1}$$

- Multiplicando ambos miembros por se obtiene $(X^n + 1)$:

$$X^i U(X) = q(X)(X^n + 1) + \underbrace{U^{(i)}(X)}_{\text{remainder}}$$

- O, de forma equivalente, en términos de aritmética modular:

$$U^{(i)}(X) = X^i U(X) \bmod (X^n + 1)$$

- Consideremos la expresión anterior para el caso $i = 1$:

$$\begin{aligned} U(X) &= u_0 + u_1 X + u_2 X^2 + \dots + u_{n-2} X^{n-2} + u_{n-1} X^{n-1} \\ XU(X) &= u_0 X + u_1 X^2 + u_2 X^3 + \dots + u_{n-2} X^{n-1} + u_{n-1} X^n \end{aligned}$$

- Sumando y restando u_{n-1} (en aritmética módulo 2 esta operación equivale a sumar u_{n-1})

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Códigos Cíclicos

□ $U^{(1)}(X)$ es de grado $n - 1$ por tanto no es divisible por $(X^n + 1)$, por tanto, resulta:

$$\frac{XU(X)}{X^n + 1} = u_{n-1} + \frac{U^{(1)}(X)}{X^n + 1} \Rightarrow U^{(1)}(X) = XU(X) \bmod (X^n + 1)$$

□ Por extensión se obtiene la expresión general:

$$U^{(i)}(X) = X^i U(X) \bmod (X^n + 1)$$

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Códigos Cíclicos

- ❑ Es posible generar un código cíclico utilizando un polinomio generador $g(X)$:

$$g(X) = g_0 + g_1X + g_2X^2 + \dots + g_pX^p$$

- ❑ Donde $g_0 = g_p = 1$
- ❑ Cada polinomio de código en el subespacio es de la forma $U(X) = m(X)g(X)$, donde $U(X)$ es un polinomio de grado menor o igual a $n - 1$ y $m(X)$ es un polinomio que representa el mensaje:

$$m(X) = m_0 + m_1X + m_2X^2 + \dots + m_{n-p-1}X^{n-p-1}$$

- ❑ Existen 2^{n-p} polinomios de código y 2^k posibles vectores de código. A cada vector de código va asociado un solo polinomio de código $\Rightarrow n - p = k$ o, de forma equivalente, $p = n - k$
- ❑ Por consiguiente, el polinomio generador $g(X)$ debe ser de grado $n - k$ y cada polinomio de código que representa un código cíclico (n, k) puede expresarse como:

$$U(X) = (m_0 + m_1X + m_2X^2 + \dots + m_{k-1}X^{k-1})g(X)$$

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Cartagena99

Códigos Cíclicos

- ❑ Un polinomio generador $g(X)$ de un código cíclico (n, k) es un factor de (X^n+1) , es decir, $(X^n+1)=g(X) h(X)$
- ❑ Por ejemplo:

$$(X^7 + 1) = (1 + X + X^3)(1 + X + X^2 + X^4)$$

- ❑ Si escogemos $g(X)=(1+X+X^3)$ (es decir el polinomio de grado $n - k=3 \Rightarrow k= n-3=4$) es posible generar un código cíclico $(7, 4)$
- ❑ Si escogemos $g(X)=(1+X+X^2+X^4)$ (es decir el polinomio de grado $n - k=4 \Rightarrow k= n-4=3$) es posible generar un código cíclico $(7, 3)$
- ❑ $g(X)$ es un polinomio de grado $n - k$, es un factor de (X^n+1) y puede generar de forma unívoca un código cíclico (n, k)

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Códigos Cíclicos

- Un mensaje de k bits $\mathbf{m}(X)$ se representa como:

$$\mathbf{m}(X) = m_0 + m_1X + m_2X^2 + \dots + m_{k-1}X^{k-1}$$

- La operación de codificación equivale a añadir en la cola del mensaje $n-k$ bits de paridad para generar la n -tupla \mathbf{U}
- Esta operación equivale a desplazar $\mathbf{m}(X)$ de $n - k$ posiciones a la derecha en un hipotético registro de desplazamiento:

$$X^{n-k}\mathbf{m}(X) = m_0X^{n-k} + m_1X^{n-k+1} + m_2X^{n-k+2} + \dots + m_{k-1}X^{n-1}$$

- Si dividimos $X^{n-k}\mathbf{m}(X)$ por $\mathbf{g}(X)$ se obtiene:

$$X^{n-k}\mathbf{m}(X) = \mathbf{q}(X)\mathbf{g}(X) + \mathbf{p}(X)$$

- El resto $\mathbf{p}(X)$ puede expresarse como

$$\mathbf{p}(X) = p_0 + p_1X + p_2X^2 + \dots + p_{n-k-1}X^{n-k-1}$$

- O, de forma equivalente:

$$\mathbf{p}(X) = X^{n-k}\mathbf{m}(X) \bmod \mathbf{g}(X)$$

- Añadiendo $\mathbf{p}(X)$ a ambos miembros de la expresión de $X^{n-k}\mathbf{m}(X)$ y aplicando la aritmética modular se obtiene:

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Códigos Cíclicos

- El primer miembro de la ecuación anterior, es decir:

$$p(X) + X^{n-k}m(X) = p_0 + p_1X + p_2X^2 + \dots + p_{n-k-1}X^{n-k-1} + m_0X^{n-k} + m_1X^{n-k+1} + m_2X^{n-k+2} + \dots + m_{k-1}X^{n-1}$$

- representa un código (n, k) válido
- El polinomio de código corresponde al siguiente vector:

$$U = \left(\underbrace{p_0, p_1, \dots, p_{n-k-1}}_{(n-k) \text{ parity bits}}, \underbrace{m_0, m_1, \dots, m_{k-1}}_{k \text{ message bits}} \right)$$

- La codificación implica el desplazamiento y la división de un polinomio; estas operaciones se pueden realizar mediante un LFSR
- Dados dos polinomios $V(X)$ y $g(X)$ de grado m y p respectivamente (con $m \geq p$):

$$V(X) = v_0 + v_1X + v_2X^2 + \dots + v_mX^m$$

$$g(X) = g_0 + g_1X + g_2X^2 + \dots + g_pX^p$$

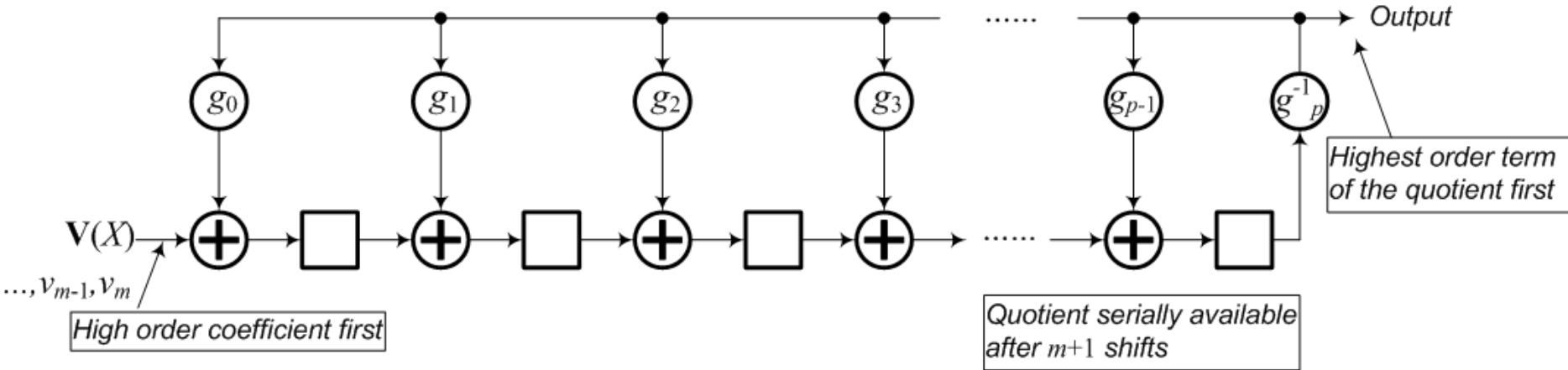
- El LFSR debe realizar la siguiente operación:

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Cartagena99

Códigos Cíclicos



Linear Feedback Shift Register (LFSR)

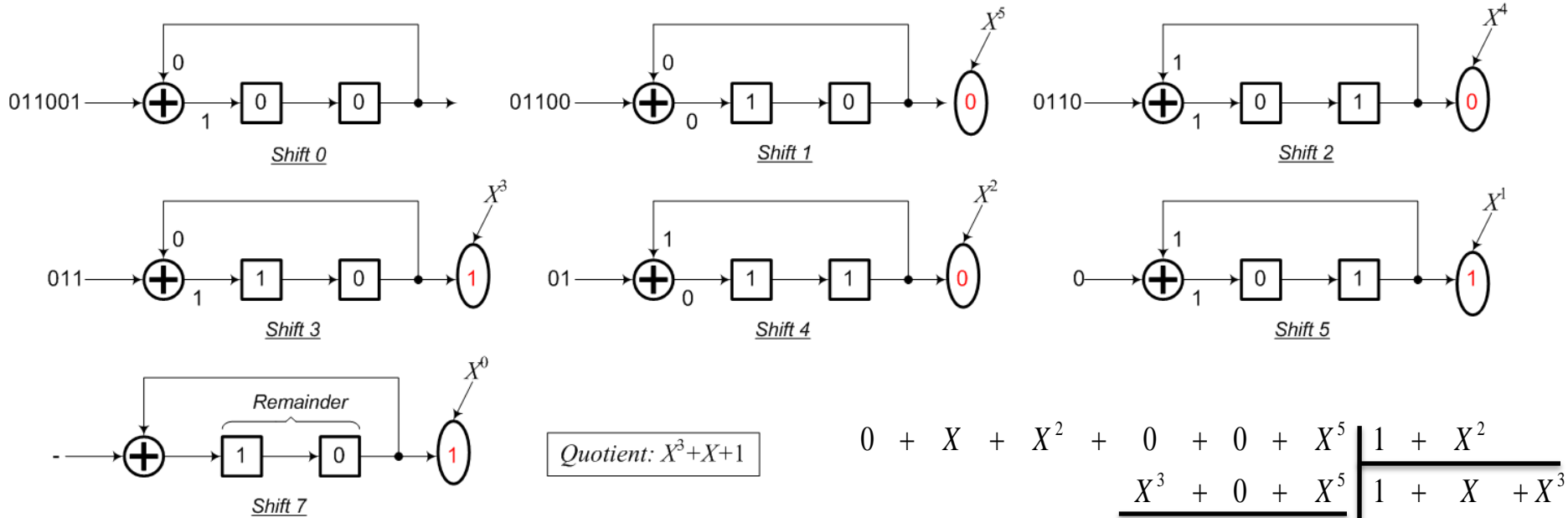
- ❑ $V(X)$ representa el mensaje desplazado hacia la derecha $X^{n-k}m(X)$
- ❑ Al terminar la división el registro de desplazamiento contiene el resto $p(X)$
- ❑ $n(X)$ representa el vector de bits de paridad que hay que añadir al

Cartagena99

CLASES PARTICULARES, TUTORIAS TECNICAS ONLINE
 LLAMA O ENVIA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
 CALL OR WHATSAPP: 689 45 44 70

Códigos Cíclicos



$$\begin{array}{r}
 0 + X + X^2 + 0 + 0 + X^5 \quad | \quad 1 + X^2 \\
 \underline{X^3 + 0 + X^5} \quad | \quad 1 + X + X^3 \\
 X^3 \quad \quad \quad // \\
 \underline{X + 0 + X^3} \quad | \\
 // \quad X^2 \quad // \\
 \underline{1 + 0 + X^2} \\
 1 \quad //
 \end{array}$$

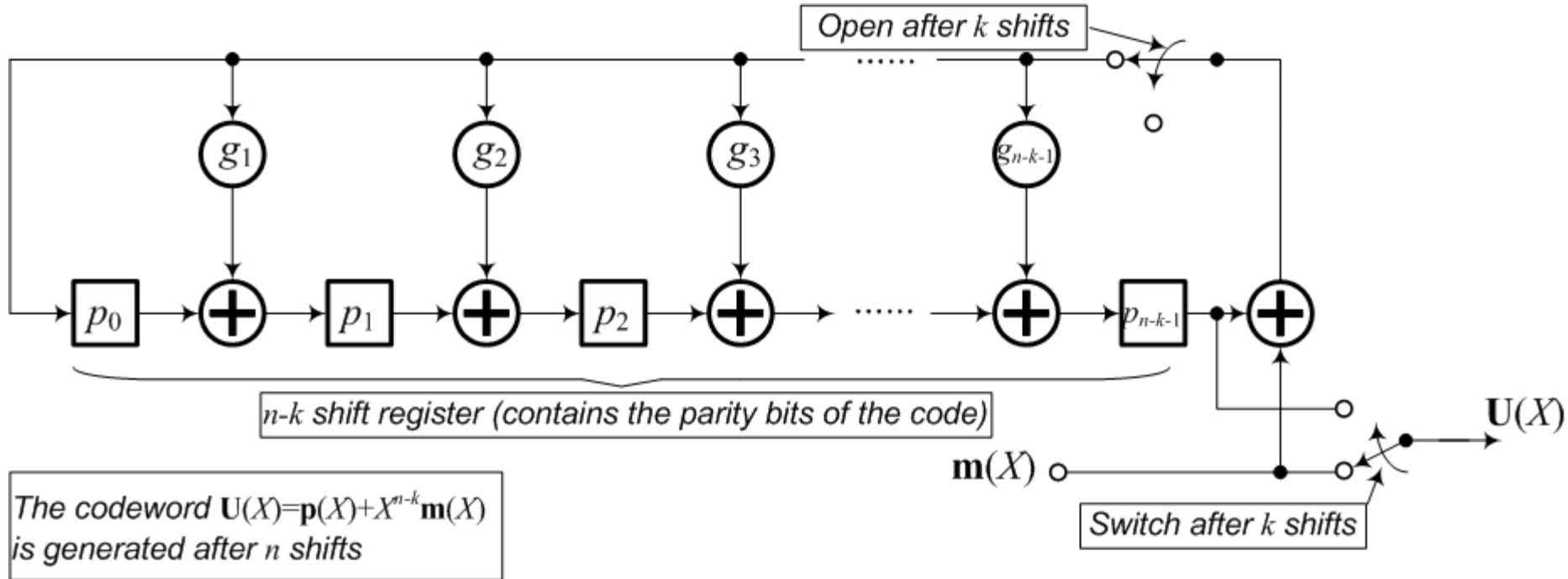
- En cada desplazamiento se calcula un dígito q_j del cociente
- El contenido del registro de desplazamiento contiene el resto parcial de la división (el resto final es su contenido después del último desplazamiento)
- La red de realimentación implementa el divisor

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
 LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
 CALL OR WHATSAPP: 689 45 44 70

Códigos Cíclicos



- ❑ En un LFSR de $n-k$ bits convencional el primer dígito válido es disponible en la salida después de $n-k+1$ desplazamientos. Por ello, para reducir el número total de desplazamientos, $m(X)$ se introduce en la etapa de salida
- ❑ Para asegurar que el término que entra en la primera etapa del LFSR sea la suma de la entrada v de la salida más significativa del LFSR, el polinomio generador $g(X)$

Cartagena99

CLASES PARTICULARES, TUTORIAS TECNICAS ONLINE
LLAMA O ENVIA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Códigos Cíclicos

- ❑ El código transmitido $U(X)$ puede estar corrompido por ruido por lo que el vector recibido $Z(X)$ es una versión corrupta del vector transmitido
- ❑ $U(X)$ es un polinomio de código por lo que es un múltiplo del polinomio generador $g(X)$, es decir:

$$U(X) = m(X)g(X)$$

- ❑ Por otro lado $Z(X) = U(X) + e(X)$ es una versión de $U(X)$ corrompida por un vector de error con representado por el polinomio $e(X)$, es decir:
- ❑ El decodificador comprueba si $Z(X)$ es un código válido, es decir, si es perfectamente divisible (con resto nulo) por $g(X)$
- ❑ Esta operación equivale a calcular el síndrome $S(X)$ del polinomio recibido:

$$Z(X) = q(X)g(X) + S(X)$$

- ❑ El síndrome es un polinomio de grado menor o igual a $n-k-1$ y puede calcularse con un LFSR
- ❑ Combinando las ecuaciones anteriores se obtiene:

$$e(X) = [m(X) + q(X)]g(X) + S(X)$$

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Códigos de Hamming

- ❑ Los códigos de Hamming son una clase muy sencilla de códigos de bloque (pertenecen a la clase de códigos perfectos) caracterizados por $(n, k)=(2^m-1, 2^m-1-m)$ con $m=2,3,\dots$
- ❑ Estos códigos tienen una distancia mínima igual a 3 por los que sólo pueden corregir errores sencillos o detectar hasta errores dobles
- ❑ El síndrome de un código de Hamming es la codificación binaria de la posición del bit erróneo en el vector recibido
- ❑ Asumiendo un decodificador con decisión firme la probabilidad de error de bit P_B de un código de Hamming es:

$$P_B \approx p - p(1-p)^{n-1}$$

- ❑ Donde p es la probabilidad de transición en un canal binario simétrico
- ❑ La relación E_c/N_0 entre energía de símbolo codificado y ruido para una señal BPSK demodulada coherentemente en un canal Gaussiano es:

$$\frac{E_c}{N_0} = \frac{2^m - 1 - m}{2^m - 1} \frac{E_b}{N_0}$$

- ❑ Es posible generalizar los códigos de Hamming para corregir también errores múltiples

Cartagena99

CLASES PARTICULARES, TUTORIAS TECNICAS ONLINE
LLAMA O ENVIA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70