Comunicaciones Digitales

Práctico 10

Codificación de canal: códigos cíclicos

Cada ejercicio comienza con un símbolo el cuál indica su dificultad de acuerdo a la siguiente escala: ✦ básica, ★ media, ✷ avanzada, y ✹ difícil.

✦ Ejercicio 1

Sea $g(X) = 1 + X + X^3$:

(a) Demostrar que se trata del polinomio generador válido de un código $C(7, 4)$.

(b) Obtenga una tabla con cada una de las palabras de código válidas.

★ Ejercicio 2

Dado un polinomio generador $g(X)$, el algoritmo para obtener un código en su forma sistemática es el siguiente:

i. Multiplicar la palabra de código a codificar $u(X)$ por X^{n-k}.

ii. Obtener el resto $b(X)$ (los dígitos de paridad) de dividir $X^{n-k}u(X)$ entre $g(X)$.

iii. Cada una de las palabras de código correspondientes será $c(X) = b(X) + X^{n-k}u(X)$

(a) Probar que el algoritmo anterior efectivamente logrará un código $C(n, k)$ en su forma sistemática.

(b) Obtener la forma sistemática del código del ejercicio anterior.

(c) ¿Qué capacidades de detección y corrección de errores tendrá este código? Obtener una tabla con los síndromes para cada patrón de error posible.

★ Ejercicio 3

Sea $g(X) = 1 + X^2 + X^4 + X^6 + X^7 + X^{10}$:

(a) Mostrar que se trata del polinomio generador de un código cíclico $C(21, 11)$

(b) Sean las sigueintes palabras de código recibidas:

- (00011110100000001000),
- (10000100000000001000),
- (00101010110010000000),

computar su síndrome y determinar si pertenecen al código o no.

✷Ejercicio 4

Mostrar que el único código $C(21, 11)$ es el generado por $g(X) = 1 + X^2 + X^4 + X^6 + X^7 + X^{10}$, pero que si existe otro código $C(7, 4)$ además del generado por $g(X) = 1 + X + X^3$.

Solución

Ejercicio 1

(a) En el teórico hemos visto que todo polinomio generador de un código cíclico $c(n,k)$ es un factor de $1+X^n$. Además, todo polinomio de grado $n-k$, que además es factor de $1+X^n$, genera un código $c(n,k)$.

Siendo entonces $g(X) = 1+X+X^3$ un polinomio de grado $7-4=3$, solo resta comprobar que además sea un factor de $1+X^7$.

$$
\begin{array}{llll|l}
1 & +X^7 & & & 1+X+X^3 \\
\cline{5-5}
X^4 & +X^5 & +X^7 & & X^4+X^2+X+1 \\
\cline{1-3}
1 & +X^4 & +X^5 & & \\
X^2 & +X^3 & +X^5 & & \\
\cline{1-3}
1 & +X^2 & +X^3 & +X^4 & \\
X & +X^2 & +X^4 & & \\
\cline{1-3}
1 & +X & +X^2 & & \\
1 & +X & +X^2 & & \\
\cline{1-3}
0 & & & &
\end{array}
$$

(b) Es posible obtener dicha tabla simplemente multiplicando cada uno de los mensajes posibles por $g(X)$

Mensaje	Palabra de Código	Polinomio
(0000)	0000000	$0 = 0 \cdot g(X)$
(1000)	1101000	$1+X+X^3 = 1 \cdot g(X)$
(0100)	0110100	$X+X^2+X^4 = X \cdot g(X)$
(1100)	1011100	$1+X^2+X^3+X^4 = (1+X) \cdot g(X)$
(0010)	0011010	$X^2+X^3+X^5 = X^2 \cdot g(X)$
(1010)	1110010	$1+X+X^2+X^5 = \left(1+X^2\right) \cdot g(X)$
(0110)	0101110	$X+X^3+X^4+X^5 = \left(X+X^2\right) \cdot g(X)$
(1110)	1000110	$1+X^4+X^5 = \left(1+X+X^2\right) \cdot g(X)$
(0001)	0001101	$X^3+X^4+X^6 = X^3 \cdot g(X)$
(1001)	1100101	$1+X+X^4+X^6 = \left(1+X^3\right) \cdot g(X)$
(0101)	0111001	$X+X^2+X^3+X^6 = \left(X+X^3\right) \cdot g(X)$
(1101)	1010001	$1+X^2+X^6 = \left(1+X+X^3\right) \cdot g(X)$
(0011)	0010111	$X^2+X^4+X^5+X^6 = \left(X^2+X^3\right) \cdot g(X)$
(1011)	1111111	$1+X+X^2+X^3+X^4+X^5+X^6$ $= \left(1+X^2+X^3\right) \cdot g(X)$
(0111)	0100011	$X+X^5+X^6 = \left(X+X^2+X^3\right) \cdot g(X)$
(1111)	1001011	$1+X^3+X^5+X^6$ $= \left(1+X+X^2+X^3\right) \cdot g(X)$

Ejercicio 2

(a) Cada palabra de código a codificar tendrá a lo sumo grado $k-1$. Por lo tanto, $X^{n-k}u(X)$ tendrá a lo sumo grado $n-1$.

La palabra $X^{n-k}u(X)$ puede o no pertenecer al código $c(n,k)$ generado por $g(X)$. En cualquier caso, su síndrome $s(X)$ deberá tener a lo sumo grado $n-k-1$.

Por construcción, $X^{n-k}u(X)$ podrá tener coeficientes positivos únicamente en $X^{n-k}, ..., X^{n-1}$. Además, como $s(X)$ es el resto de dividir $X^{n-k}u(X)$ entre $g(X)$ se cumple que $X^{n-k}u(X) = g(X)q(X) + s(X)$, o lo que es lo mismo $X^{n-k}u(X) + s(X) \in c(n,k)$.

(b) Usando el algoritmo de la parte anterior se obtiene la siguiente tabla.

Mensaje	Palabra de Código	Polinomio
(0000)	(0000000)	$0 = 0 \cdot g(X)$
(1000)	(1101000)	$1 + X + X^3 = g(X)$
(0100)	(0110100)	$X + X^2 + X^4 = Xg(X)$
(1100)	(1011100)	$1 + X^2 + X^3 + X^4 = (1 + X)g(X)$
(0010)	(1110010)	$1 + X + X^2 + X^5 = \left(1 + X^2\right) g(X)$
(1010)	(0011010)	$X^2 + X^3 + X^5 = X^2 g(X)$
(0110)	(1000110)	$1 + X^4 + X^5 = \left(1 + X + X^2\right) g(X)$
(1110)	(0101110)	$X + X^3 + X^4 + X^5 = \left(X + X^2\right) g(X)$
(0001)	(1010001)	$1 + X^2 + X^6 = \left(1 + X + X^3\right) g(X)$
(1001)	(0111001)	$X + X^2 + X^3 + X^6 = \left(X + X^3\right) g(X)$
(0101)	(1100101)	$1 + X + X^4 + X^6 = \left(1 + X^3\right) g(X)$
(1101)	(0001101)	$X^3 + X^4 + X^6 = X^3 g(X)$
(0011)	(0100011)	$X + X^5 + X^6 = \left(X + X^2 + X^3\right) g(X)$
(1011)	(1001011)	$1 + X^3 + X^5 + X^6 = \left(1 + X + X + X^2 + X^3\right) g(X)$
(0111)	(0010111)	$X^2 + X^4 + X^5 + X^6 = \left(X^2 + X^3\right) g(X)$
(1111)	(1111111)	$1 + X + X^2 + X^3 + X^4 + X^5 + X^6$ $= \left(1 + X^2 + X^5\right) g(X)$

(c) Al obtener toda la tabla vemos que la distancia mínima del código es 3. Por lo tanto es capaz de corregir $\left\lfloor \frac{D_{min}-1}{2} \right\rfloor = 1$ bit errado por palabra.

Como $r = X + e$, los patrones de error que estamos en condiciones de corregir son:

Patrón de Error $e(X)$	Síndrome s(X)	Vector Síndrome (s_0, s_1, s_2)
$e_6(X) = X^6$	$s(X) = 1 + X^2$	(101)
$e_5(X) = X^5$	$s(X) = 1 + X + X^2$	(111)
$e_4(X) = X^4$	$s(X) = X + X^2$	(011)
$e_3(X) = X^3$	$s(X) = 1 + X$	(110)
$e_2(X) = X^2$	$s(X) = X^2$	(001)
$e_1(X) = X^1$	$s(X) = X$	(010)
$e_0(X) = X^0$	$s(X) = 1$	(100)

Ejercicio 3

(a) Siendo $g(X)$ un polinomio de grado $1-k = 21-11 = 10$, si probamos que además es factor de $1 + X^{21}$ sabremos entonces que es generador de un código $c(21, 11)$

$$
\begin{array}{llllllll|l}
1 & +X^{21} & & & & & & & 1+X^2+X^4+X^6+X^7+X^{10} \\
\cline{9-9}
X^{11} & +X^{13} & +X^{15} & +X^{17} & +X^{18} & +X^{21} & & & X^{11}+X^8+X^7+X^2+1 \\
\cline{1-6}
1 & +X^{11} & +X^{13} & +X^{15} & +X^{17} & +X^{18} & & & \\
X^8 & +X^{10} & +X^{12} & +X^{14} & +X^{15} & +X^{18} & & & \\
\cline{1-6}
1 & +X^8 & +X^{10} & +X^{11} & +X^{12} & +X^{13} & +X^{14} & +X^{17} & \\
X^7 & +X^9 & +X^{11} & +X^{13} & +X^{14} & +X^{17} & & & \\
\cline{1-6}
1 & +X^7 & +X^8 & +X^9 & +X^{10} & +X^{12} & & & \\
X^2 & +X^4 & +X^6 & +X^8 & +X^9 & +X^{12} & & & \\
\cline{1-6}
1 & +X^2 & +X^4 & +X^6 & +X^7 & +X^{10} & & & \\
1 & +X^2 & +X^4 & +X^6 & +X^7 & +X^{10} & & & \\
\cline{1-6}
0 & & & & & & & &
\end{array}
$$

(b) En cada caso tenemos:

- $r_1(X) = X^3 + X^4 + X^5 + X^6 + X^8 + X^{17}$
- $r_2(X) = 1 + X^5 + X^{17}$
- $r_3(X) = X^2 + X^4 + X^6 + X^8 + X^9 + X^{12}$

Podemos observar que $r_3(X) = X^2 g(X)$, por lo tanto es directo ver que pertenece al código.

Si calculamos para $r_2(X)$ obtenemos:

$$
\begin{array}{llllllll|l}
1 & +X^5 & +X^{17} & & & & & & 1+X^2+X^4+X^6+X^7+X^{10} \\
\cline{9-9}
X^7 & +X^9 & +X^{11} & +X^{13} & +X^{14} & +X^{17} & & & X^{11}+X^8+X^7+X^2+1 \\
\cline{1-6}
1 & +X^5 & +X^7 & +X^9 & +X^{11} & +X^{13} & +X^{14} & & \\
X^4 & +X^6 & +X^8 & +X^{10} & +X^{11} & +X^{14} & & & \\
\cline{1-6}
1 & +X^4 & +X^5 & +X^6 & +X^7 & +X^8 & +X^9 & +X^{10} & +X^{13} \\
X^3 & +X^5 & +X^7 & +X^9 & +X^{10} & +X^{13} & & & \\
\cline{1-6}
1 & +X^3 & +X^4 & +X^6 & +X^8 & & & & \\
\end{array}
$$

Vemos entonces que $r_2(X) = g(X)q(X) + s(X)$ y por lo tanto $r_2(X) + s(X) \in C$

Finalmente, tenemos que $r_1(X) = X^3 + X^4 + X^5 + X^6 + X^8 + X^{17} = (1 + X^5 + X^{17}) + (1 + X^3 + X^4 + X^5 + X^6 + X^8) = r_2(X) + s(X)$ y por lo tanto se cumple que $r_1(X) \in C$.

Ejercicio 4

Por ejercicio 3 parte (a) sabemos que:
$1 + X^{21} = (1 + X^2 + X^4 + X^6 + X^7 + X^{10})(1 + X^2 + X^7 + X^8 + X^{11})$

Por lo tanto, no existe otro polinomio de grado $n - k = 21 - 11 = 10$ que sea factor de $1 + X^n = 1 + X^2 1$. Entonces no existe otro código $c(21, 11)$ que el generado por $g(X) = 1 + X^2 + X^4 + X^6 + X^7 + X^{10}$.

Por otro lado, a partir de lo obtenido en el ejercicio 1 parte (a) tenemos que:
$1 + X^7 = (1 + X + X^3)(1 + X + X^2 + X^4)$
$1 + X^7 = (1 + X + X^3)(1 + X^2 + X^3)(1 + X)$

Por lo tanto, existe otro polinomio de grado $n - k = 7 - 4 = 3$ que sea factor de $1 + X^n = 1 + X^7$. Es decir, existe otro código cíclico $c(7, 4)$ de polinomio generador $g(X) = 1 + X + X^3$.